RESUMEN

El presente trabajo se remite expresamente a la problemática sobre Delitos Informáticos, para la creación y la correcta aplicación e interpretaciones de las normas penales, que como ya se dijo anteriormente la diferencia única con los delitos tradicionales, es el medio utilizado, el modus operandi; respetando las estructuras constitucionales y del andamiaje jurídico de la legislación.

En este trabajo, se establecen generalidades y algunas consideraciones asociadas al fenómeno, la conceptualización de los Delitos Informáticos y Delitos Electrónicos como base y guía para su correcta interpretación y entendimiento; así como las conductas de los ciber-criminales, para luego pasar a Delimitar el Fenómeno de la Delincuencia Informática.

Además se aborda las Nuevas Formas de Delinquir en la Era Informática, que dado su carácter multifacético y su previsible intensidad e impacto en el mediano y largo plazo ha generado estas nuevas formas criminales cuyos efectos de esta revolución digital o era tecnológica se hacen sentir en los distintos sectores de la sociedad: economía y finanzas, política, educación, cultura, deportes, etc.

Por otro lado, se estudiará y analizará a los Ciber-Delincuentes y sus clases, que apareció en un primer momento únicamente como una “aventura o juego”, motivados por el desafío técnico o la curiosidad. Pero que luego surgió el perfil "transgresor" y actualmente se verifican motivaciones delictivas de envergadura, obteniendo cuantiosos e innumerables beneficios económicos, valiéndose de la ingenuidad de los cibernautas y sus técnicas para vulneras las seguridades de la Red, un simple ejemplo los falsos antivirus.

Para finalizar se estudiará y analizará de manera objetiva y en cierto modo técnicamente, como poder minimizar la amenaza de los delitos a través de la seguridad, con tres sistemas considerados actualmente los más eficientes y seguros, como son: La **Firma Electrónica**, cuya utilización puede garantizar la integridad del mensaje, su reconocimiento y autenticación; tratada en la Ley

67[1] de nuestra legislación; **PGP (Pretty Good Privacy)** su objetivo es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, siendo su función principal "esconder información" a ojos de otras personas que quieran tener acceso a ella; **SSL (Secure Socket Layer)**, protocolo de seguridad cuya misión es cifrar los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico de clave pública y clave privada, para evitar la manipulación de información confidencial. Como es obvio, siempre existen bienes que tutelar y proteger; es así que al termino de este capítulo se aborda el tema de los bienes jurídicos protegidos en el delito informático, es decir, "el bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido".

Palabras Claves: Ciber-Delincuentes, Delitos Informáticos, Delitos Electrónicos, tecnología, Fraude Informático, Criminalidad Informática

[1] ***Ley 67.-*** *Ley de Comercio electrónico, firmas electrónicas y mensajes de datos, art. 13 y siguientes.*

INDICE GENERAL

HACIA UNA CORRECTA HERMENÉUTICA PENAL: DELITOS INFORMÁTICOS VS. DELITOS ELECTRÓNICOS

Introducción 11

CAPÍTULO I
DELITOS INFORMATICOS Y DELITOS ELECTRÓNICOS

1.1. Algunas Consideraciones 16
1.2. Conceptualización y generalidades 20
1.3. Delimitación del Fenómeno de la Delincuencia Informática 27
1.3.1. Delincuencia Informática y Abuso Informático 30
1.3.2. Criminalidad Informática 33
1.4. Delitos informáticos vs. Delitos Electrónicos 34

CAPÍTULO II
NUEVAS FORMAS DE DELINQUIR EN LA ERA TECNOLÓGICA

2.1. Introducción 50
2.2. El Delito Informático 51
2.3. Los Ciber-Delincuentes: Un Lucrativo Negocio 56
2.3.1. Quienes son los Ciber-Delincuentes 60
2.3.2. Clases de Ciber-Delincuentes 63
2.4. La Ciber-Criminalidad 64
2.4.1. El Sabotaje Informático 69
2.4.2. Acceso no Autorizado a Servicios Informáticos 70
2.4.3. El Fraude Informático 71
2.4.4. El Espionaje Informático 72
2.4.5. El Robo de Servicios 73
2.5. Infracciones que no Constituyen Delitos Informáticos 74
2.6. El Delito Informático y su realidad Procesal en el Ecuador 74

CAPITULO III

IMPACTO DE LOS DELITOS INFORMÁTICOS

3.1. Impacto a Nivel General 79

3.2. Impacto a Nivel Social 82

3.3. Impacto en la Esfera Judicial 85

3.4. Impacto en la Identificación de Delitos a Nivel Mundial 87

CAPITULO IV

SEGURIDAD CONTRA LOS DELITOS INFORMÁTICOS

4.1. Seguridad en Internet 94

4.2. Firma Electrónica 101

4.3. P.G.P 112

4.4. SSL Secure Socket Layer 116

4.5. Los Bienes Jurídicos Protegidos en el Delito Informático 122

Conclusiones 127

Recomendaciones 131

Bibliografía 134

Páginas Web 137

UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA, CIENCIAS POLÍTICAS Y SOCIALES

ESCUELA DE DERECHO

HACIA UNA CORRECTA HERMENEUTICA PENAL: DELITOS INFORMÁTICOS vs. DELITOS ELECTRÓNICOS

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN DERECHO INFORMÁTICO MENCIÓN EN COMERCIO ELECTRÓNICO

AUTOR: **DR. CRISTIAN HERRERA AVILA**

DIRECTOR: **DR. SANTIAGO ACURIO DEL PINO**

CUENCA-ECUADOR

2010

DEDICATORIA

Al SER que con su nacimiento colmo de felicidad y alegría mis días, con su tierna mirada, su sonrisa angelical y sus travesuras por doquier definitivamente cambiaste mi vida y para siempre; a Ti Hijo Mío: Matteo Josué, te entrego y dedico este trabajo de tesis, alcanzando así un objetivo profesional más, para que quizá con el pasar de los años sirva de guía y ejemplo a seguir lo que hoy tu padre con mucho sacrificio, dedicación y entrega pero con humildad a conseguido.

Con profundo sentimiento de Amor y Cariño, a pesar de la distancia que hoy Dios y la vida nos ha puesto, va esta mi especial dedicación para ti hijo mío; Te Adoro y Amo por siempre Matteito.

Tu Padre:

Cristian H.

Y a mi Hermano Edgar Fabián (Coco), quien a pesar de la difícil y dura prueba que Dios le puso en su vida es un modelo de lucha constante y ejemplo de superación, y que pesar de su "enfermedad" jamás se ha dado por vencido y día a día es más valiente, con fortaleza inagotable de valor, serenidad y decisión. Nunca te RINDAS Hermano Querido que Dios te ilumine; y, mi apoyo incondicional siempre.

EL AUTOR

AGRADECIMIENTO

Reconocimiento y gratitud, son grandes valores y virtudes que el hombre lleva en su ser desde siempre; más sin embargo, no por mostrarme que soy un hombre lleno de virtudes, debo reconocer el inmenso sacrificio, apoyo incondicional y "lucha" constante que mis padres Julio Eduardo y Julia Leonor; han depositado y confiado en mí, su hijo Cristian Eduardo, para alcanzar los objetivos y triunfos profesionales hasta hoy conseguidos; así como en todos los aspectos de mi vida. Siendo los pilares fundamentales en el convivir diario.

Vaya pues mi eterno y profundo agradecimiento, a mis queridos Padres, que como es natural con la bendición y encomendado en el Ser Supremo Dios, a mi amigo que nunca me ha fallado Mi Divino Niño, en brazos de mi madre del cielo que con su manto Divino me ha protegido Virgen de la Nube; he culminado una etapa académica mas, con dedicación y humildad; para de alguna manera devolver y recompensar todo lo hecho por mis padres para que se sientan orgullosos de su hijo.

Mi especial agradecimiento a mi Director de Tesis Dr. Santiago Acurio del Pino, quien de una manera desinteresada tuvo la gentil

aceptación para guiarme a la consecución de este Trabajo, con sus amplios y experimentados conocimientos siendo un profesional a carta cabal.

EL AUTOR

RESPONSABILIDAD

Todos los comentarios, expresiones y manifiestos plasmados en el presente trabajo de tesis, en forma íntegra son de mi total Autoría y Responsabilidad.

Dr. Cristian Herrera Ávila

Autor

Certifico que la presente tesis

es elaborada en su totalidad

por el Dr. Cristian Herrera Ávila,

como autor de la misma.

Dr. Santiago Acurio del Pino

DIRECTOR DE TESIS

INTRODUCCIÓN

A lo largo de nuestra historia hemos transcurrido por diferentes etapas, cada una de ellas han presentando rasgos o particularidades especiales que las caracterizaron. Actualmente, estamos viviendo en la Era de la Informática, en la Era del mundo globalizado o simplemente en la "Era Digital", donde la información es el mayor centro de atención y en ella están puestas todas las miradas.

Por lo tanto, a nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales y bancarias, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, salud, educción, "amor", etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática que deberá estar acompañada de una eficiente seguridad.

Sin embargo, junto al avance vertiginoso de esta maravillosa tecnología y su influencia en todas las áreas de la vida social, han surgido una serie de comportamientos ilícitos, dañinos, "atípicos" e "inimputables", denominados de manera genérica Delitos Informáticos.

La problemática que me ocupa entonces no es "distinta en cierto modo de los delitos tradicionales", pues lo único que diferencia unos de otros es el medio, la herramienta, el espacio utilizado, el modus operandi; ya que mientras los Delitos Informáticos y solo por citar un ejemplo, para la comisión del acto delictivo se realiza utilizando una computadora para robar miles de dólares en un banco; en los Delitos Tradicionales el Sujeto Activo del delito utiliza una arma de fuego para robar este banco.

El derecho y la tecnología en los últimos años han contribuido significativamente a que la sociedad de un giro total en el desarrollo de su vida,

y esto ha dado como resultado que en el campo del derecho se agregue una nueva ciencia jurídica como es la **Informática Jurídica**, considerada como una ciencia jurídica propia y que puede ser estudiada independientemente de las otras ciencias jurídicas; y, el **Derecho Informático.**

Lamentablemente el progreso de la técnica en general y de la informática en particular no han sido acompañados de defensas adecuadas que permitan hacer frente a la mala utilización de las mismas. Me refiero específicamente a los distintos ordenamientos jurídicos o derechos que deben responder a los nuevos y complejos problemas que se originan como consecuencia de este fenómeno universal.

La inexistencia de regulación legal específica y el anonimato que se produce en el ciber-espacio, son factores criminológicos que favorecen el desarrollo, expansión y proliferación de delitos cometidos a través de los medios electrónicos, creándose situaciones atípicas en la que los principios de legalidad y tipicidad impiden el juzgamiento y las sanciones correspondientes.

Con estos breves pero necesarios exordios, en este trabajo se realiza un desarrollo hermenéutico de los términos Delitos Electrónicos y Delitos Informáticos, a fin de establecer su correcta interpretación legal, que como es sabido muchas veces dista de la común. De igual manera se intentará dar soluciones y mecanismos de derecho eficientes para lograr su tipicidad y penalización. Así como técnicas informáticas de seguridad para precautelar la integridad de los mensajes de datos y todo lo que conlleva el Comercio Electrónico y la Red de Redes.

En el Primer Capítulo se establecen generalidades y algunas consideraciones asociadas al fenómeno, la conceptualización de los Delitos Informáticos y Delitos Electrónicos como base y guía para su correcta interpretación y entendimiento; así como las conductas de los ciber-criminales, para luego pasar a Delimitar el Fenómeno de la Delincuencia Informática, definida como “todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal,

dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera"; al final de este capítulo se estudia de manera muy objetiva y profunda los Delitos Informáticos y Delitos Electrónicos, que para una mejor comprensión e interpretación del tema se establecen semejanzas y diferencias, características y la ley aplicable, para de esta manera llegar una correcta hermenéutica penal y jurídica.

En el Segundo Capítulo se aborda las Nuevas Formas de Delinquir en la Era Informática, que dado su carácter multifacético y su previsible intensidad e impacto en el mediano y largo plazo ha generado estas nuevas formas criminales cuyos efectos de esta revolución digital o era tecnológica se hacen sentir en los distintos sectores de la sociedad: economía y finanzas, política, educación, cultura, deportes, etc. Se analizará el Delito Informático, entendido como: "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[2]. Por otro lado, se estudiará y analizará a los Ciber-Delincuentes y sus clases, que apareció en un primer momento únicamente como una "aventura o juego", motivados por el desafío técnico o la curiosidad. Pero que luego surgió el perfil "transgresor" y actualmente se verifican motivaciones delictivas de envergadura, obteniendo cuantiosos e innumerables beneficios económicos, valiéndose de la ingenuidad de los cibernautas y sus técnicas para vulneras las seguridades de la Red, un simple ejemplo los falsos antivirus. Todo asociado en este mismo capítulo con las formas de ciber criminalidad de que se valen los delincuentes informáticos, así como aquellas infracciones que no constituyen Delitos Informáticos, concluyendo este capítulo con la legislación ecuatoriana y su realidad procesal en torno al tema que, en la actualidad aún falta mucho para tipificar, sancionar y penalizar estos "nuevos actos delictivos", ya que estos no están recogidos en el actual Código Penal con mayor énfasis y atención, implicando un serio y grave riesgo de caer en la atipicidad y por ende en la impunidad.

[2] *Definición dado por* ***María Luz de Lima***

Se menciona estadísticas mundiales sobre delitos informáticos, casos más representativos y sonados de los últimos años, así como el impacto de éstos en diferentes áreas a Nivel General, Social, Judicial, etc.; esto en el Capítulo Tercero.

Para finalizar esta tesis en el Capítulo Cuarto, se estudiará y analizará de manera objetiva y en cierto modo técnicamente, como poder minimizar la amenaza de los delitos a través de la seguridad, con tres sistemas considerados actualmente los más eficientes y seguros, como son: La **Firma Electrónica**, cuya utilización puede garantizar la integridad del mensaje, su reconocimiento y autenticación; tratada en la Ley 67[3] de nuestra legislación; **PGP (Pretty Good Privacy)** su objetivo es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, siendo su función principal "esconder información" a ojos de otras personas que quieran tener acceso a ella; **SSL (Secure Socket Layer)**, protocolo de seguridad cuya misión es cifrar los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico de clave pública y clave privada, para evitar la manipulación de información confidencial. Como es obvio, siempre existen bienes que tutelar y proteger; es así que al termino de este capítulo se aborda el tema de los bienes jurídicos protegidos en el delito informático, es decir, "el bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido".

Al final del documento se establecen las conclusiones pertinentes al estudio, en las que se busca destacar situaciones relevantes, comentarios, análisis, etc. Así como algunas recomendaciones en torno al tema, muy especialmente en el ámbito de la administración de justicia, esto debido a que, el avance vertiginoso de esta "era digital, han surgido varios inconvenientes, vacios y oscuridades legales a la hora de aplicar la ley respecto de los delitos informáticos. Esto porque, muchos de los juzgadores desconocen en lo absoluto estas "nuevas figuras delictivas, y la forma de aplicar la ley".

[3] ***Ley 67.-*** *Ley de Comercio electrónico, firmas electrónicas y mensajes de datos, art. 13 y siguientes.*

En resumen, el presente trabajo se remite expresamente a la problemática sobre Delitos Informáticos, para la creación y la correcta aplicación e interpretaciones de las normas penales, que como ya se dijo anteriormente la diferencia única con los delitos tradicionales, es el medio utilizado, el modus operandi; respetando las estructuras constitucionales y del andamiaje jurídico de la legislación.

CAPÍTULO I

DELITOS INFORMÁTICOS Y DELITOS ELECTRÓNICOS

1.1. Algunas Consideraciones

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, ubicándolas así como un nuevo medio de comunicación condicionando su desarrollo a la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. Ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido muy generalmente como la "Era de la Información o la Era Digital".

Junto con el nacimiento del Comercio Electrónico ha hecho su aparición la delincuencia en línea. El crimen ha encontrado en los medios tecnológicos nuevas estrategias para avanzar en sus intenciones, aprovechando las vulnerabilidades relativas a las tecnologías informáticas y las fallas comunes de los procesos organizacionales. El uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta surgen algunas facetas negativas, como por ejemplo, lo que ya se conoce como «Criminalidad Informática».

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunas de las tácticas relacionadas con el procesamiento electrónico de datos mediante los cuales se obtienen grandes beneficios económicos o causan importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así

ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

He aquí entonces, los serios inconvenientes que se presentan para la administración de justicia respecto de cuál es la norma aplicable para el caso concreto, y cuál será su correcta interpretación judicial, en base a las normas no específicas, ni claras menos aún expresas en torno a este "Delito Informático".
Una explicación objetiva y jurídica de lo hasta aquí mencionado sería que, el delito es una conducta de acción u omisión típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible; y que supone una infracción al Derecho penal, es decir, penada por la ley. El Delito Informático se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

De la definición expuesta se concluye entonces que este nuevo delito reúne todas las características del delito en general; y las únicas diferencias es el medio, método o herramienta utilizada para su cometimiento. Entonces si este delito informático, reúne dichas características, su sanción y punibilidad dependerá de la "**Correcta Interpretación Judicial**[4]**"** que haga o pueda hacer el juzgador al momento de aplicar la ley penal; pues la norma legal para este caso ya existe solo ha cambiado quizá "su figura literal", es decir, Delito-Informático.

Aspecto importante es que, los criminales informáticos se manifiestan en varios modelos de perfiles individuales o grupales, pero que tienen en común el gusto por las tecnologías y sus posibilidades, que sirviéndose del absoluto desconocimiento de un gran porcentaje de personas, diseñan estrategias para

[4] ***Interpretación Judicial.-*** *Es la actividad que llevan a cabo los jueces y magistrados en el ejercicio de la diligencia jurisdiccional que les está encomendada, consistente en determinar el* ***sentido y alcance*** *de las normas jurídicas.*

lograr sus ilícitos, violando las seguridades, garantías y derechos de los cibernautas que utilizan las tecnologías de la información de una manera adecuada, correcta y sin buscar el perjuicio de los demás.

No existe una precisa definición o perfil específico de estos delincuentes. Se mencionan varias características: unos orientados por las tecnologías y sus avances, otros por la inestabilidad emocional y con problemas para definir los límites de sus impactos y actuaciones, otros con ánimo de lucro y beneficios personales. Desde esta perspectiva, cualquier persona puede convertirse en delincuente informático, bastaría solo una motivación, el medio obviamente que será el tecnológico y el momento preciso para actuar.

La delincuencia en Internet, también llamada Delincuencia Cibernética, es toda actividad ilícita derivada de uno o más componentes de Internet, como sitios en la web, salas de tertulia (chat rooms) o correo electrónico. Esta delincuencia abarca desde el incumplimiento en la entrega de bienes o servicios y la intrusión en ordenadores, al uso indebido del derecho de propiedad intelectual, el espionaje electrónico[5], la extorsión en línea, el blanqueo internacional de dinero, el robo de identidad y una lista cada vez mayor de otros delitos facilitados por internet.

En el mundo virtual al igual que en el mundo real, las actividades criminales son iniciadas mayormente por individuos o grupos pequeños y se las puede entender mejor como "crímenes desorganizados". Pero hay pruebas crecientes de que existen grupos de crimen organizado que explotan ilícitamente y con ánimo de lucro las oportunidades ofrecidas por Internet. El crimen organizado y el crimen cibernético nunca serán sinónimos. El primero seguirá actuando mayormente en el mundo real y en el mundo cibernético; y, el segundo será perpetrado por individuos y no por organizaciones criminales.

[5] ***Espionaje electrónico.-*** *Robo o comercio de secretos.*

En el IC3[6] de Fairmont-Virginia Occidental, 6 agentes federales y unos 40 analistas de la industria y de instituciones académicas reciben denuncias por delitos cometidos a través de Internet presentadas por el público, denuncias que una vez tramitadas son remitidas a organismos federales, estatales, locales e internacionales de ejecución de la ley o agencias reguladoras para su investigación. En el sitio de la web www.ic3.gov se pide el nombre, la dirección y el número de teléfono del denunciante; el nombre, la dirección y el número de teléfono y la dirección en la web, en su caso, de la persona u organización de quien se sospecha es responsable de alguna actividad delictiva; detalles de cómo, por qué y cuándo se cree que una persona ha cometido un delito y cualquier otra información que respalde la denuncia.

El principal objetivo operativo del IC3 es recibir la denuncia de un ciudadano particular que pueda representar un delito causante de daños por un valor de por ejemplo: 100 dólares, y combinarlo con información de otras 100 o 1.000 víctimas de todo el mundo que han perdido dinero por la misma estratagema, y establecer un caso importante a la mayor brevedad. Un delito cibernético casi nunca tiene una sola víctima. Así pues, los investigadores del IC3 pueden vincular denuncias afines y transformarlas en un caso de 10.000 ó 100.000 dólares, con 100 ó 1.000 víctimas; entonces el delito pasa a ser un asunto importante y las agencias de ejecución de la ley lo pueden investigar.

Ahora bien, el presente trabajo de tesis intentará dar una pauta para una mejor comprensión de lo que debe entenderse, en primer término por Delito Informático y/o Delito Electrónico, y, en segunda instancia la ley aplicaba para el caso en cuestión; a través de una Correcta Hermenéutica Penal y Jurídica abordada desde un punto de vista legal, doctrinal y auténtica en base a todo lo investigado y analizado.

---

[6] ***ICE3.-*** *El Internet Crime Complaint Center del FBI es un centro de coordinación de denuncias individuales de actividades delictivas en línea. El IC3 correlaciona la información de centenares de víctimas del mismo tipo de fraude y establece un caso importante, de cuyo procesamiento se encargarán los organismos de ejecución de la ley.*

Así entonces expuestas las consideraciones, creo que es muy conveniente definir lo que es la Hermenéutica Penal y Jurídica, para que en base a estas descripciones se tenga una idea clara y objetiva de esta "Nueva Figura Delictiva" en la **Era Digital;** y no caer en susceptibilidades vanas de incomprensión o confusión.

Para **Guillermo Cabanellas de Torres,** en su Diccionario Jurídico Elemental **Hermenéutica** es: "Ciencia que interpreta los textos escritos y fija su verdadero sentido a una referida primeramente exégesis bíblica, se relaciona con más frecuencia a la interpretación jurídica". Entonces la Hermenéutica Penal sería la interpretación de normativas legales del Derecho Penal. Dejando puntualizado que el presente trabajo no se limita únicamente al ámbito penal, por ende será también una Hermenéutica o Interpretación Jurídica, es decir, una interpretación de los textos legales, manejo de los conceptos, nociones y dogmas del Derecho. En definitiva se hará una correcta Hermenéutica o Interpretación de los términos Delitos Informáticos y/o Delitos Electrónicos, en base a los criterios de la doctrina, legislación nacional e internacional, convenciones internacionales y demás documentos de soporte que en el desarrollo del trabajo se podrá apreciar.

1.2. Conceptualización y Generalidades

Quizá para quien no haga del derecho penal una práctica habitual y constante, y para quienes no profundizan sus estudios y análisis respecto del inmenso espectro del Internet, no encuentren alguna diferencia o la necesidad de definir estos dos términos: **Delitos Informáticos y Delitos Electrónicos,** que hoy en día en lenguaje común y aún en el de algunos medios especializados en torno al tema resultan sinónimos.

Para una mejor comprensión de estas dos expresiones, formularé en primera instancia y de manera general lo que es la Electrónica e Informática, para así apriori determinar o no una diferencia entre ambas terminologías.

"Electrónica: Estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos, por ejemplo: computador, tarjeta, pantalla, etc.

Informática: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores[7]. Conceptualmente, se entiende como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores (computadoras), con el fin de almacenar, procesar y transmitir información y datos en formato digital[8].

Corresponde tras referenciar la significación idiomática de aquellas analizar el marco conceptual en que ambos términos son utilizados: **"por medio de" y "en contra de".**

Antes primero se advierte, que todos los equipos informáticos están construidos con elementos electrónicos, pero no todos los equipos electrónicos son necesariamente equipos informáticos, ejemplo: radio o televisor. También se advierte que sólo los equipos con la capacidad de procesar datos pueden ser utilizados como medio comisivo de acciones ilícitas que afecten bienes jurídicos protegidos, pues resulta difícil imaginar a un sujeto activo tratando, por ejemplo, violar una cerradura electrónica de un banco usando una radio o un celular (equipos electrónicos no informáticos), pero es fácil imaginar al mismo sujeto activo intentando igual acción por medio de un equipo portátil de procesamiento de datos u otro similar con la capacidad de generar infinidad de claves numéricas[9].

Con esta breve explicación y aclaración algo particular, se podría decir e "**interpretar técnica y jurídicamente"** que hay Delitos cometidos en contra de

---

[7] ***Microsoft Encarta 2009.***
[8] ***www.wikipedia.com: Informática.***
[9] ***www.alfa-redi.org: Revista de Derecho Informático;*** *Delitos Informáticos vs. Delitos electrónicos, por: Gabriel Andrés Campoli; "La necesidad del Análisis"*

equipos electrónicos y Delitos cometidos por medio de elementos o equipos informáticos.

Para construir las bases de una sólida hermenéutica jurídica es menester en este momento describir el ámbito de aplicación de cada uno de los casos bajo análisis.

“Los delitos cometidos en contra de equipos electrónicos son aquellos en los cuales el receptor físico del daño impetrado por el autor resulta expresamente un equipo electrónico”. Dentro de esta categoría no se podría, por ejemplo, incluir el delito de daños, en los casos en que alguien destruye un cajero automático, salvo que este tuviere que ver con destrucciones producidas a través de la utilización de medios informáticos.

En contraposición, están los delitos cometidos por medio de elementos informáticos, los cuales presentan una variada gama de lesiones a bienes jurídicos protegidos, están daños, las injurias y calumnias, las estafas, etc.

De esta **“aparente diferencia”,** hay una quizá más sutil pero dígase científica y porque no jurídica, ¿Cuál es el bien jurídico protegido en cada caso? En el primero se advierte que es la integridad física y lógica de los equipos electrónicos, y por ende el derecho de propiedad del sujeto pasivo, en el segundo en cambio advertimos que son múltiples las posibilidades de bienes jurídicos a proteger y altamente disímiles entre sí como el honor, la protección de datos, el patrimonio, derecho a la intimidad, imagen y buen nombre, propiedad intelectual, acceso no autorizado a la información, espionaje informático, etc.

Determinado el bien jurídico protegido, en el caso de los delitos informáticos, los múltiples posibles ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales.

¿Entonces qué es lo que nos separa de una correcta aplicación de las leyes penales preestablecidas? Sólo la pretendida falta de legislación en materia de

delitos informáticos, y digo pretendida porque esto no es así, ya que al perpetrarse el delito a través del uso de medios informáticos, simplemente se está en presencia de un nuevo método comisivo del delito y no como erróneamente se piensa de un nuevo delito que para que lo sea debe estar correctamente tipificado. Más aún, hoy en día y de acuerdo a las últimas reformas al Código Penal, Ley 67 y otras que en el transcurso de estas tesis analizaré, regulan y legislan estos delitos, sin embargo, y es preciso anotar que aún falta mucho a nuestro normativa jurídica por establecer regulaciones y sanciones en torno al tema en estudio.

En resumen, los delitos informáticos en su gran mayoría dependen para su investigación y procedimiento judicial de la correcta interpretación de la ley penal, así como la concientización de los jueces de que sólo nos encontramos ante **"nuevos métodos"** para estafar o para injuriar, pero en ningún caso ante nuevos delitos. Solo a manera de referencia o explicación objetiva: incoherente sería imaginar que si mañana se pudiese quitar la vida a alguien por medio de internet habría que establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica[10].

En el ámbito específico de los delitos electrónicos, nos encontramos frente a un caso de delito de daños, por regla general no existe legislación en la materia. Para estos casos es que se requiere una rápida acción del legislador para definir los tipos penales y agregarlos a los vigentes, sin perjuicio de que al hacer las respectivas modificaciones y según la legislación de cada país puedan agravarse algunos tipos existentes en función del uso de nuevas tecnologías para de esta forma desalentar su utilización indebida.

---

[10] ***www.alfa-redi.org: Revista de Derecho Informático;*** *Delitos Informáticos vs. Delitos electrónicos, por: Gabriel Andrés Campoli; "La necesidad del Análisis".*

Luego de haber analizado detenidamente las consideraciones expuestas anteriormente y mediante una interpretación jurídica[11], y siguiendo la recomendación del Dr. Santiago Acurio del Pino en la que manifiesta: la interpretación jurídica no es monopolio exclusivo de los órganos aplicadores del derecho, sino de cualquier persona que dote de significado al lenguaje jurídico, puede realizar una interpretación jurídica; por lo tanto según este comentario objetivo y legal me permito sostener que: "**todos los delitos electrónicos son perpetrados por medio del uso de la informática, razón por la cual vendrían hacer una especie del género de los Delitos Informáticos";** en forma análoga como lo es la Firma Electrónica el género de la Firma Digital que es la especie**.**

Así expuestas las consideraciones es importante tener en cuenta las siguientes definiciones a fin de evitar confusiones en la hermenéutica penal.

Delitos Informáticos: Son aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente de cada país, pudiendo ser de diverso tipo por medio de la utilización indebida de medios informáticos.

Delitos electrónicos o informáticos electrónicos: son una especie del género delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios.

De lo dicho, y a manera de conclusión respecto de este tema, puedo afirmar luego de una Hermenéutica Penal y Jurídica existe desde un punto de vista personal y legal solo Delitos Informáticos, que los delitos electrónicos son únicamente una especie de aquellos, y que al final de cuentas lesionan un bien jurídico sea o no protegido por la legislación nacional. Y respecto

---

[11] *La **interpretación jurídica (o del derecho)** es una actividad que consiste en establecer el significado o alcance de las normas jurídicas y de los demás estándares que es posible encontrar en todo ordenamiento jurídico y que no son normas, como por ejemplo, los principios.*

de este tema la NO conceptualización del Delito Informático así como su **"aparente inexistencia de sanción"** en nuestra legislación ecuatoriana hace que se dé su imputabilidad, sin embargo, quiero referirme brevemente pero muy objetivo diciendo que: **"… 6.- En los casos en que no pudiere aplicarse la reglas de interpretación precedentes, se interpretarán los pasajes oscuros o contradictorios del modo que mas conforme aparezca al espíritu general de la legislación y la equidad natural; y, 7.- A falta de ley, se aplicarán las que existan sobre casos análogos; y no habiéndolas, se ocurrirá a los principios del derecho universal"[12].**

Es decir, que bajo ningún concepto e interpretación puede el juzgador argumentar que para la perseguibilidad, trámite y sanción a un sujeto activo del Delito Informático, necesita de una ley nueva y específica, pues lo único que ha variado en torno a este Delito, es el medio utilizado nada más y eso es lo único que dista de los delitos tradicionales.

Entonces cuando hablamos de delitos informáticos estamos en presencia de una acción u omisión socialmente peligrosa, prohibida por ley bajo la conminación de una sanción penal. Al igual que en el resto de los delitos existe un sujeto activo (que no se habla de delincuentes comunes, sino de personas especializadas en tecnología) y otro pasivo. El hecho de que no sea considerado el sujeto activo delincuente común está determinado por el mecanismo y medio de acción que utilice para llegar a producir el daño, quiénes en la mayoría de los supuestos en que se manifiestan y las funciones que desempeñan pueden ser catalogados sujetos especiales.

Delitos Informáticos cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos[13].

Existen delincuentes de la informática que pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar

---

[12] ***Título Preliminar, parágrafo 4º. Interpretación Judicial de la Ley,*** *art. 18 Reglas de interpretación de la ley, numerales 6 y 7 del Código Civil ecuatoriano en vigencia.*
[13] *Definición tomada de WORDPRESS, Realidad Alternativa: El Delito Informático.*

con daños a los sistemas con el fin de cometer extorsión, ya sea directamente o mediante los llamados "gusanos" o "virus", que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

En sentido amplio se podría definir el delito informático como "toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena"[14].

Julio Téllez Valdez señala que los delitos informáticos son «actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)».

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son: "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo"

En definitiva, los delitos informáticos tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos, utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático: hardware o software.

Los delincuentes informáticos son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro. Los ataques amenazan la creciente y substancial confianza del comercio, gobierno y público en la infraestructura de la información para realizar negocios, enviar mensajes y procesar información; esto hace que se cuestionen los asuntos de riesgo y reputación de la marca.

[14] ***www.mailxmail.com:*** *Curos de Delitos Informáticos.*

Las conductas perjudiciales que se efectivizan utilizando el medio informático en general obedecen a los siguientes factores: **Familiares:** El nivel social al que pertenecen los sujetos que invaden el mundo informático es de medio a alto, provienen de una extracción que les pudo proporcionar estas herramientas para alcanzar las metas que la cultura social les estaba proponiendo. Así el acceso a esta tecnología no es propio de zonas marginales. **Sociales:** el progreso tecnológico de las comunicaciones permitieron transacciones que, en segundos conllevaron a un mayor poder económico y político extranacional. Cuando surge el auge de la informática es notorio que todo aquél que desconoce el manejo de una computadora cae en la obsolencia así como considerado un “analfabeto digital”.

Ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y particulares, con rapidez y ahorro de tiempo y energía, configuran un cuadro de realidades de aplicación y de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social. La informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que se conoce como «criminalidad informática o delincuencia informática».

1.3. Delimitación del Fenómeno de la Delincuencia Informática

Actualmente se habla de las nuevas formas de delincuencia informática. De ahí que, importante es medir el crecimiento de la utilización de estos medios informáticos en la vida económica de un estado y poder dimensionar la trascendencia de dichos medios, y la incidencia en la vida delictual, para así poder establecer con claridad cuáles son los medios utilizados, cual es el daño causado, en que campo interfiere, cual es la conducta típica, y

fundamentalmente si realmente existe una norma legal que tipifique estas conductas[15].

El descubrimiento y la utilización práctica de la Informática, marcó un hito en el mundo, dando lugar a que se hable de un antes y un después de la computadora y la informática. Pero hay algo que nadie planeó, algo que se escapó a la mente de los creadores de estos descubrimientos revolucionarios, que es "La Delincuencia Informática. Por lo que, es tiempo de delimitar los alcances de las diversas conductas y establecer un tamiz de condiciones que nos permitan tener aunque sea una mínima seguridad en la utilización de estos medios informáticos. Y siendo el Derecho un instrumento regulador por excelencia de las actividades sociales, no debe mantenerse al margen ni realizar una negación de este fenómeno mundial de la informática.

Gutiérrez Francés[16] señala que puede hablarse de "criminalidad o delincuencia informática" como categoría exclusivamente criminológica y de carácter funcional, para aludir en forma conjunta a los problemas que las nuevas tecnologías presentan al ordenamiento penal.

Se podría decir que: "Delincuencia Informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera"[17].

Sin duda alguna, el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para mucha clase de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato.

---

[15] ***Diego Leonardo Lindow,*** *alumno de la Universidad Católica de Santiago del Estero; Delito Informático: Legislación, Represión y Prevención.*

[16] ***Protección contra la Delincuencia Informática en el MERCOSUR,*** *por Marcelo Alfredo Riquert; Universidad Nacional de Mar del Plata*

[17] **Dr. Santiago Acurio del Pino,** del Ministerio Público de Pichincha; Delitos Cibernéticos y Cibercriminalidad.

Los alcances de la Delincuencia Informática, es una fuente inagotable de hechos, sujetos y fundamentalmente de medios para la comisión de diversos *delitos independientes*[18], pero que utilizan para su comisión medios informáticos. Por ejemplo, delitos cometidos con las tarjetas de crédito, entre una infinidad de modalidades.

En la Delincuencia Informática existe un **Sujeto Pasivo ó Víctima del delito,** ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, portales de ventas de bienes y servicios, redes sociales (hi5-facebook), etc., que usan sistemas automatizados de información conectados a otros. Es importante saber y conocer al sujeto pasivo, con el objeto de prever las acciones antes mencionadas, pues muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos, y que no son denunciados a las autoridades competentes, sumado a la falta de leyes que protejan a las víctimas de estos delitos, falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas; hace que la delincuencia informática se mantenga bajo la llamada "cifra oculta" o "cifra negra". **Sujeto Activo ó Delincuente Informático,** es aquella persona o grupo de personas que, valiéndose de medios informáticos, tecnológicos y de la ingenuidad, desconocimiento de la tecnología y uso de internet del sujeto pasivo, vulnera un bien jurídico protegido. Por cierto, el delincuente informático se perfecciona en distintos perfiles, características, objetivos y especialidades, serán más adelante abordados.

Teniendo en cuenta las características de las personas que cometen los "delitos informáticos" el criminólogo Edwin Sutherland lo ha catalogado como

---

[18] ***Delitos Independientes.-*** *existencia de 2 o más acciones que estén tipificadas como delitos independientes, ligadas por una relación de medio a fin, que obedezca a una conexidad teleológica.*

"delitos de cuello blanco"[19]. Entre las características que posee el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, carencia de recreación, baja educación, poca inteligencia, inestabilidad emocional, sino por el simple hecho del cometimiento.

1.3.1. Delincuencia Informática y Abuso Informático

Sin duda alguna, la **"delincuencia informática", "Ciberdelincuencia" o "Cybercrimen"** constituye uno de los máximos exponentes de las nuevas realidades delictivas.

GÓMEZ PERALS define como: "conjunto de comportamientos dignos de reproche penal que tienen por instrumento u objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

La Comunicación define la delincuencia informática en sentido amplio, como "todo delito que implique la utilización de las tecnologías informáticas". Esto hace referencia a: la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y, a la circulación de datos intangibles y volátiles[20]. En ella concurren el empleo de las nuevas tecnologías y la producción de riesgos antes desconocidos e impensados, por ejemplo, nuevas formas de ataque a la intimidad, defraudaciones de cuantías elevadas, abuso informático, espionaje informático, acceso no autorizado a la información, etc.; y su carácter transfronterizo y susceptibilidad a la comisión por bandas organizadas[21].

---

[19] ***Delitos de Cuello Blanco.-*** *o white collar crimen, actos delincuenciales que se caracterizan por la violación de la ley, cometidas por personas de nivel socio-económico elevado, en el cuadro de sus actividades profesionales y por la obtención considerada de ganancias. Se cometen mediante la utilización de la malicia, engaño o falseamiento, para crear y explotar la apariencia de una transacción legítima con el fin de obtener un beneficio de carácter ilícito. Presenta gran variedad de apariencias, desde los vertidos tóxicos al espionaje industrial, incluye el delito cometido por funcionarios y agencias estatales.*

[20] ***europa.eu:*** *Europa, Actividades de la Unión Europea síntesis de la Legislación: Lucha contra la Delincuencia Organizada-Lucha contra los Delitos Informáticos.*

[21] ***Párrafo,*** *tomado de JESUS MARIA SILVA SÁNCHEZ, del trabajo realizado por Juan José González López, Artículos Doctrinales: Derecho Informático; noticias.jurídicas.com*

La delincuencia informática es difícil de comprender o conceptualizar plenamente. A menudo, se la 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.

La delincuencia informática actúa bajo varios tipos, que atacan a las propias tecnologías de la información y las comunicaciones, como los servidores y los sitios Web, con virus informáticos de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores. El vandalismo electrónico y la falsificación profesional. El robo o fraude, por ejemplo, ataques de piratería contra bancos o sistemas financieros y fraude mediante transferencias electrónicas de fondos. La “pesca” (phishing) o la inundación de mensajes supuestamente de origen conocido (Spam y Spoofing) es la construcción de mensajes de correo electrónico con páginas Web diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que se anuncian como provenientes de bancos, subastas en línea u otros sitios “legítimos” para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas. Otro motivo de preocupación es la pornografía infantil. Desde fines de los años 80, ha venido aumentando su distribución a través de una infinidad de redes informáticas, utilizando una variedad de servicios de Internet, incluidos los sitios Web. Una cierta proporción de la distribución de pornografía infantil se ha vinculado a la delincuencia organizada transnacional. Además de la utilización de la Internet para difundir propaganda y materiales que fomentan el odio y la xenofobia, hay indicios de que la Internet se ha utilizado para facilitar la financiación del terrorismo y la distribución de propaganda terrorista. Son algunos tipos de entre una extensa gama de delitos informáticos.

El Abuso Informático o Abuso del Ordenador es “Cualquier incidente asociado con la tecnología de ordenadores en el cual una víctima sufrió o pudo

haber sufrido pérdidas, y el que lo ocasiona, tuvo o pudo haber tenido beneficio"[22].

Las tecnologías, incluyendo las computadoras, generan nuevos artículos que robar, nuevas formas de robarlos y nuevas maneras de dañar a los demás. El delito informático es la ejecución de actos ilegales mediante el uso de una computadora o contra un sistema de cómputo, estas pueden ser el objeto del delito (destruyendo el centro de cómputo o los archivos de cómputo de una compañía), así como el instrumento de un delito (el robo de listas de una computadora mediante un acceso ilegal al sistema de cómputo utilizando una computadora casera). El *Abuso Informático,* es la ejecución de actos que implican una computadora, que tal vez no sean ilegales pero que se consideran inmorales.

Tradicionalmente, los empleados –internos- han sido el origen de la mayoría de daños y abusos informáticos porque tienen el conocimiento, acceso y frecuentemente un motivo relacionado con el puesto para cometer tales delitos. Una forma muy difundida de Abuso Informático es el spamming[23]. Algunas leyes estatales prohíben o restringen el spamming pero no está regularizado (lamentablemente en nuestra legislación ni siquiera existe una ley completa para este tipo de delitos). Un aspecto importante a considerar es que, el Parlamento Europeo con fecha 30 de mayo del 2002, aprobó una iniciativa sobre el envío de mensajes comerciales no solicitados. El marketing electrónico solo puede tener como objetivo a personas que hayan dado antes su consentimiento.

---

[22] ***lalasoylala.blogspot.com:*** *Abuso Informático*

[23] ***Spamming.-*** *Se llama* ***Spam****,* ***correo basura*** *o* ***sms basura*** *a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades e incluso masivas que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. También puede tener como objetivo los teléfonos móviles, a través de mensajes de texto y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, etc. Igual a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes y pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a links en diversas páginas.*

1.3.2. Criminalidad Informática

Con la expresión "criminalidad informática se alude a todos los actos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos o computadora"[24]. Baón Ramírez, criminalidad informática es la realización de un tipo de actividades tipificadas como delito, llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

La criminalidad informática puede afectar bienes jurídicos tradicionalmente protegidos por el ordenamiento penal, delitos en los que se utiliza el computador para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, la fe pública o la seguridad nacional. En otros casos, las conductas del agente van dirigidas a lesionar bienes no protegidos tradicionalmente por la legislación penal, por ejemplo: los Bienes Informáticos, consistentes en datos, información computarizada, archivos y programas insertos en el soporte lógico del ordenador. En este tipo de conductas disvaliosas se encuentran entre otros el fraude electrónico y el sabotaje informático.

A nivel de organizaciones Intergubernamentales de carácter mundial, en el seno de la Organización de las Naciones Unidas, en el marco del Octavo Congreso sobre prevención del delito y justicia Penal", celebrado en 1990 en la Habana-Cuba, se señaló que la criminalidad informática era producto del mayor empleo de procesos de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Los criminales informáticos o vándalos electrónicos en su generalidad son de sexo masculino, de 18 a 30 años de edad, con características de ser un empleado de confianza en la empresa en la que labora, posee necesariamente conocimientos técnicos en computación. El animus delicti de estos agentes, es

[24] ***www.alfa-redi.org-****Revista de Derecho Informático: Los Delitos Informáticos; por Julio Núñez Ponce.*

motivado por razones de carácter lucrativo, por la popularidad que representa este actuar en la sociedad moderna o por simple diversión ¨hackers¨, o por la intención de que su actuar puede responder al deseo de destruir o dañar un sistema informático, desestabilizando el normal desenvolvimiento en la institución o empresa ¨crackers¨. Ambos causan perjuicios al sistema informático, lo que varia es la intencionalidad en su comisión.

La regulación jurídica de la criminalidad informática presenta determinadas peculiaridades, debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan. En el plano de la Dogmática Jurídico-penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales, obligando a revisar los elementos constitutivos de gran parte de los tipos penales existentes.

1.4. Delitos Informáticos vs. Delitos Electrónicos

Durante el transcurso del tiempo y desde la proliferación del Internet y desde la creciente expansión vertiginosa de conductas atentatorias contra los derechos del sujeto pasivo que lesión un bien jurídico protegido, se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", etc. Sin embargo, no existe una definición universal propia del Delito Informático y/o Electrónico; en razón de que su misma denominación alude a una situación muy especial, pues al hablar de “delitos”, es decir, de acciones tipificadas o contemplados en textos jurídicos penales, se requiere que la expresión “delitos informáticos y/o electrónicos” este consignada en los códigos penales, lo cual en nuestra legislación no ha sido objeto de tipificación, haciendo aún más complejo estás acciones criminógenas.

“Delito: Electrónico y/o Informático?

La doctrina mayoritaria define al **Delito Informático** como aquella conducta en la cual el medio comisivo es la utilización propia de un sistema informático. Sin embargo, esta idea es demasiado genérica, pues el empleo en sí mismo de un

sistema informático, no es determinante para conceptualizar el término, toda vez que al hacerlo, se incurriría en el error de definir como "*delito informático*" a todas aquellas conductas en donde intervenga un sistema informático[25].

Delito Electrónico es todo acto que infringe la ley y que se realiza aplicando algún medio de procesamiento electrónico, por ejemplo: el robo a un banco violando la seguridad de algún sistema electrónico de información (censores, cámaras, puertas eléctricas, etc.), el robo a un cajero automático violando el artefacto físicamente no es delito electrónico. Sin embargo, una violación de la seguridad del cajero utilizando tarjetas falsas precodificadas, si lo tipifica como tal, porque viola la forma electrónica de la seguridad del cajero[26].

Los términos Electrónica e Informática son utilizados en marcos conceptuales diferentes que, aunque de ellos no se extraiga una delimitación exacta, se distinguen dos causales disímiles en donde desembocar en torno al tema: **"en contra de" y "por medio de".**

A saber, "delitos" cometidos:

1. **En contra de sistemas electrónicos:** son aquellos en los cuales el receptor físico del daño resulta ser un sistema electrónico y el bien jurídico protegido es el patrimonio del sujeto pasivo, NO todos los sistemas electrónicos son sistemas informáticos (radio, televisor, celular, teléfono convencional).
2.
3. **Por medio de sistemas informáticos:** los cuales están dotados de capacidad para procesar datos, por ende son utilizados como herramientas comisivas de acciones que afecten bienes jurídicos protegidos, por ejemplo: la violación de un sistema informático de seguridad por medio de otro sistema similar o compatible de

[25] ***YOSHI, Toranaga;*** *Fundamentos teóricos-doctrinarios de los Delitos Electrónicos, 25 enero 2008.*
[26] ***SALOM, Genaro y ARTEGA, Valentín,*** *Delitos Electrónicos-Complicación.*

procesamiento de datos (software), con la capacidad de descubrir los passwords o datos para ingresar a él[27].

La jurisconsulta María de la Luz Lima define:

"El **delito electrónico** en sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la **tecnología electrónica** sea como método, medio o fin; y, en sentido estricto, **el delito informático**, cualquier acto ilícito penal en el que **las computadoras**, sus técnicas y funciones desempeñan un papel como método, medio o fin."

En la definición que antecede se hace una distinción entre el delito electrónico y delito informático. El primero no se circunscribe a la existencia o no de computadoras, sino más bien al empleo de la tecnología electrónica. Ejemplos de estos delitos: la desviación del tráfico de llamadas (*By-pass*), uso fraudulento de tarjetas de crédito, etc. Mientras que el delito informático, implica la utilización de una computadora para su realización.

Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. **Como instrumento o medio*:*** conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo: falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc. Variación de la situación contable. Alteración al funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
2. **Como fin u objetivo:** conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física, por ejemplo: instrucciones que producen un bloqueo parcial o total del sistema. Destrucción de programas por cualquier método. Atentado físico contra la computadora, sus accesorios o sus medios de

[27] ***PEÑA Pérez, Pascal A.,*** *Delitos Electrónicos: Necesidad de una Ley que sancione los Crímenes y Delitos de Alta Tecnología en República Dominicana; Seminario "Delitos Informáticos en la R. D." INTEC – 29 de Marzo, 2005*

comunicación. Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos":

1. **Como Método:** conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. **Como Medio:** conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. **Como Fin:** conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Las acciones que más tipifican los delitos electrónicos son:

- Espionaje de comunicaciones, clave de la mayoría de delitos electrónicos.
- Interferencia de comunicaciones por vía telefónica utilizadas con más frecuencia en fraudes con tarjeta de crédito, chantajes, espionaje industrial, etc.

Los delitos más conocidos dentro de la familia delictiva denominad delito electrónico, esta:

- Fraudes con tarje de crédito en las transferencias electrónicas, especialmente en los cajeros automáticos, mismos que se cometen violando los sistemas electrónicos de criptografía (PIN).
- Estafas en los procesos de pagos on-line en las transacciones comerciales por violación de los códigos de seguridad, por robo de los números de las tarjetas de crédito.
- Espionaje Internacional, Industrial y Personal manipulación de la información.

Otros delitos frecuentes de esta clase son.

- Problemas técnicos, por ejemplo daño en el firewalle,

- Virus electrónico
- Engaños y estafas por correo electrónico

De lo expuesto se extrae el siguiente cuadro comparativo referente a los delitos informáticos y los delitos electrónicos, dejando sentado como premisa que se ha obtenido lo más importante y objetivo en torno al tema:

DELITOS INFORMÁTICOS **SEMEJANZAS** **DELITOS ELECTRÓNICOS**	
Utilizan la tecnología más avanzada en su esencia o incluso la inventan. Violentan las seguridades de terceros por distintos medios y métodos.	
Para la comisión de estos delitos siempre se utiliza la Informática. Nuestra legislación no conceptualiza ninguna de estas figuras delictivas. Los dos delitos atentan contra bienes jurídicos protegidos por la ley.	
Ambos tipos de delitos tienen ánimo de lucro y beneficio personal. Para su penalización y sanción depende de una correcta hermenéutica penal, pues en derecho, si hay lesión en un bien jurídico cualquiera no importa cuál sea el medio utilizado.	
Estos delitos implican una acción u omisión socialmente peligrosa prohibida por la ley, bajo la conminación de una sanción penal. Existe tanto sujeto activo como pasivo, expertos y especialista en esta tecnología.	
No se trata de nuevos delitos, sino de nuevas formas de ejecutar las figuras típicas tradicionales, mismas que están ya configuradas en la legislación de cada país.	
DIFERENCIAS	
Todos los equipos informáticos son construidos con elementos electrónicos.	No todos los equipos electrónicos son equipos informáticos.
Delitos cometidos por medio de elementos o equipos informáticos configuran D Informático	Hay delitos en contra de quipos electrónicos y por ende configuran el Delito Electrónico.
La Tutela del bien jurídico protegió es variado, ej. Acceso no autorizado-Derecho a la Intimidad	El bien jurídico protegido atentado es el Derecho a la Propiedad-Delito de Daños.
Son cometidos por medio de elementos o equipos informáticos, con valor agregado: Internet haciendo más simple y fácil.	Perpetrados utilizando la informática, y no se circunscribe a la existencia o no de computadoras sino a la tecnología electrónica.
Solo los equipos con capacidad de procesar datos son utilizados como medio comisivo de actos ilícitos	No todos los equipos electrónicos sirven para cometer actos criminales. Este delito es una especie de los Delitos Informáticos.
Acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin	Conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin.

<table>
<tr><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td>Utiliza tecnología informática. Para su cometimiento es necesario un elemento o equipo informático</td><td>Usa tecnología electrónica. No siempre el medio para el acto delictivo es una computadora.</td></tr>
<tr><td>Son acciones ocupacionales, muchas veces se realizan cuando el sujeto se halla trabajando.</td><td>Su acción criminológica puede ser en distintos momentos con o sin presencia del S. Pasivo.</td></tr>
<tr><td>Ofrecen posibilidades de tiempo y espacio, en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.</td><td>Atenta contra un bien jurídico “especifico” Derecho a la Propiedad.</td></tr>
<tr><td colspan="2">Son conductas criminales de cuello blanco (White collar crime), puesto que sólo un determinado número de personas con ciertos conocimientos (técnicos) puede llegar a cometerlas.</td></tr>
<tr><td colspan="2">Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación específica por parte del Derecho.</td></tr>
<tr><td colspan="2">Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.</td></tr>
<tr><th colspan="2">LEY APLICABLE</th></tr>
<tr><td colspan="2">Respecto a este tema e insistiendo en las tantas veces ya dicho de que, “no estamos ante nuevas figuras delictivas, sino ante nuevas formas de cometer delitos tradicionales; es menester profundizar objetivamente a este respecto, y lo hago en las siguientes consideraciones:

Determinado el bien jurídico protegido, en el caso de los delitos informáticos, los múltiples posibles ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales. De la misma manera para el caso de los delitos electrónicos –insisto, especie tan solo de los D. Informáticos-, que el bien jurídico protegido en este caso que es la propiedad, está ya tipificado en los cuerpos legales de nuestra legislación.

De acuerdo a la Constitución Política de la República, en su Título IV, Capitulo 4to, en la sección décima, Art. 195 señala que: “La Fiscalía dirigirá, de oficio o a petición de parte la investigación pre procesal y procesal penal……”. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala “el ejercicio de la acción pública corresponde exclusivamente al fiscal”. De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal.
Es por tanto el Fiscal quien deberá llevar la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente.</td></tr>
</table>

Los delitos que aquí se describen se encuentran como reforma al Código Penal en la Ley de Comercio Electrónicos, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67. Registro Oficial. Suplemento 557 de 17 de Abril del 2002.

DELITOS CONTRA LA INFORMACIÓN PROTEGIDA: VIOLACIÓN DE CLAVES O SISTEMAS DE SEGURIDAD

CÓDIGO PENAL	DESCRIPCIÓN
Título II: DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL. Capítulo V. De los Delitos Contra la inviolabilidad del secreto.	**Art. … (202.1).-** Delitos contra la información protegida. **Art. … (202.2).-** Obtención y utilización no autorizada de información.
LEY DE COMRCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 58.-** Delitos contra la información protegida.
CONCORDANCIAS	
CAPITULO VI: Derechos de Libertad Constitución Política. CAPÍTULO VII: De la Información no Divulgada. Ley de Propiedad Intelectual	**Art. 66.-** Derechos de Libertad numerales 19 y 20. **Art. 186**.- Responsables de la Infracción **Art. 316**.- Secretos comerciales o información confidencial.

DELITOS CONTRA LA INFORMACIÓN PROTEGIDA: DESTRUCCIÓN O SUPRESIÓN DE DOCUMENTOS, PROGRAMAS.

CÓDIGO PENAL	DESCRIPCIÓN
TITULO III. DE LOS DELITOS CONTRA LA ADMINISTRACION PÚBLICA. Capítulo V De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad.	**Art. … (257.3).-** Aprovechamiento indebido de información reservada. **Art. 262.-** Destrucción maliciosa de documentos.
LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 59.-** Destrucción maliciosa de documentos
CONCORDANCIAS	
Título II Capítulo II, Sección 3ª. Comunicación e Información-C. Política	**Art. 20.-** Cláusula de conciencia, secreto profesional y reserva de fuente.

FALSIFICACIÓN ELECTRÓNICA

CODIGO PENAL	DESCRIPCIÓN
Título IV. DE LOS DELITOS CONTRA LA FE PUBLICA.- Capítulo III. De las Falsificaciones de Documentos en General	**Art. … (353.1).-** Falsificación Electrónica
LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 60.-** Falsificación electrónica
CONCORDANCIAS	
Título I Capítulo I, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.	**Art. 7.-** Información Original **Art. 8.-** Conservación de los mensajes de datos.

DAÑOS INFORMÁTICOS

CODIGO PENAL	DESCRIPCIÓN
Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PÚBLICA. Capítulo VII.- Del incendio y otras Destrucciones, de los deterioros y Daños	**Art. … (415.1).-** Daños Informáticos. **Art. … (415.2).-** Sanción por delito mayor.
LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICA Y MENSAJES DE DATOS	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 61.-** Daños Informáticos.

FRAUDE INFORMÁTICO

CODIGO PENAL	DESCRIPCIÓN
Titulo X. De los Delitos contra la Propiedad. Capítulo II. Del Robo Capítulo V De las Estafas y otras defraudaciones.	**Art. … (553.1).-** Apropiación Ilícita. **Art. … 563.- Estafa,** inciso segundo.
LEY DE COMERICO ELECTRÓNICO, FIRMAS ELECTRÓNICA Y MENSAJES DE DATOS.	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 62.-** Apropiación ilícita. **Art. 63.- Estafa,** inciso segundo

VIOLACIONES AL DERECHO A LA INTIMIDAD (CONTRAVENCIÓN)

CODIGO PENAL	DESCRIPCIÓN
LIBRO III. TITULO I. Capítulo III. De las contravenciones de tercera clase.	**Art. … 606.- Casos.-** numeral 20
LEY DE COMERICO ELECTRÓNICO, FIRMAS ELECTRÓNICA Y MENSAJES DE DATOS.	
TITULO V: DE LAS INFRACCIONES INFORMÁTICAS. Capítulo I. De las Infracciones Informáticas.	**Art. 57.-** Infracciones Informáticas. **Reformas al Código Penal, Art. 64.-** Contravenciones de tercera clase.
CONCORDANCIAS	
CAPITULO VI: Derechos de Libertad Constitución Política. Título I Capítulo I, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	**Art. 66.-** Derechos de Libertad numerales 20. **Art. 5.-** Confidencialidad y reserva **Art. 9.-** Protección de datos.

PORNOGRAFÍA INFANTIL

CODIGO PENAL	DESCRIPCIÓN
TITULO VIII DE LA RUFIANERÍA Y CORRUPCIÓN DE MENORES, Capítulo III.1, De los Delitos de Explotación Sexual.	**Art. … (528.7).-** Producción, comercialización y distribución de imágenes pornográficas.
CONCORDANCIAS	
LIBRO I Título IV De la protección contra el maltrato, abuso y explotación sexual, tráfico y pérdida de niños, niñas y adolescentes	**Art. 68**.- Concepto de abuso sexual. **Art. 69.-** Concepto de explotación sexual.-

Ahora bien de lo expuesto en el cuadro anterior, surge una inquietud latente para muchos “que desconocen la ley 67”, y que con la exposición siguiente se aclarará el panorama y no habrá lugar a duda alguna mucho menos a falsas interpretaciones legales, menos aún falta de ley aplicable a los casos en cuestión, respecto de las evidencias digitales y reconocimiento jurídico de los datos.

Ley 67 en su art. 2 al texto dice: "*Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterán al cumplimiento de lo establecido en esta Ley y su Reglamento".*

Con este artículo nuestra ley está reconociendo el Principio de Equivalencia Funcional, Principio elemental del comercio electrónico en "Derecho y Tecnología"; basado en un análisis de los objetivos y funciones que cumple la presentación de un escrito o documento físico, con miras a determinar la manera de satisfacer los objetivos y funciones del comercio telemático, entonces *cumple de igual forma la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado*". En otras palabras la equivalencia funcional permite aplicar a los soportes informáticos respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas: los mismos efectos jurídicos que surte con las manifestaciones de la voluntad instrumentadas a través de un documento en papel.

Por otro lado, los **Medios de prueba, el art. 52 ibídem dice:** Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

La **Validez de las actuaciones procesales por medio de las Tecnologías de la Información y Comunicación,** está consignado en el art. **147 de La Ley orgánica de la función Judicial que dice: Validez y eficacia de los documentos electrónicos.-** Tendrán la validez y eficacia de un documento físico original los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos, satelitales o producidos por nuevas tecnologías, destinadas a la tramitación judicial. Ya sea que contengan actos o resoluciones judiciales. Igualmente los reconocimientos de firmas en

documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia…
Esta disposición del Código Orgánico de la Función Judicial ratifica el principio de equivalencia funcional existente en la Ley de Comercio Electrónico.

Relevancia y Admisibilidad de la Evidencia Digital, la evidencia es la materia que usamos para persuadir al tribunal o al juez de la verdad o la falsedad de un hecho que está siendo controvertido en un juicio. Son entonces las normas procesales y las reglas del debido proceso las que informarán al juez o al tribunal que evidencias son relevantes y admisibles dentro de un proceso judicial y cuáles no lo son[28].

Miguel López Delgado[29], define la evidencia digital como "el conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencia a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado".
Por lo tanto, esta evidencia digital es un tipo de evidencia física, que pueden ser recolectados y analizados con herramientas y técnicas especiales, así como de peritos y expertos en el área.

Para esta tarea compleja y difícil, esta la Informática Forense; El FBI la conceptualiza como: "la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional". Este mismo organismo ha desarrollado programas que permiten examinar evidencia computacional.
Gerberth Adín Ramírez, identifica los objetivos de la informática forense con el fin de: perseguir y procesar judicialmente a los criminales; crear y aplicar

[28] ***ACURIO del Pino, Santiago,*** *Perfil Sobre los Delitos Informáticos en el Ecuador; documento guía para la VI Reunión del Grupo de Trabajo en Delito Cibernético de la REMJA, que se realizó el 21 y 22 de Enero del 2010 en Washington D.C.*
[29] ***DELGADO López, Miguel,*** *Análisis Forense Digital, Página 5, 2da Edición, 2007*

políticas para prevenir posibles ataques y de existir antecedentes evitar casos similares; compensar daños causados por los criminales o intrusos[30].

Esta ciencia relativamente nueva se aplica tanto para las investigaciones de delitos tradicionales como para aquellos que están estrechamente relacionas con las TIC´s, entre estas piratería de software, distribución pornográfica infantil, tráfico de bases de datos, etc.

En nuestra legislación el Fiscal General Del Estado creo mediante Acuerdo 104-FGE-2008 el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado, cuyo trabajo está centrado en lo siguiente:

1. **Identificación de incidentes.-** En ésta primera fase se debe asegurar la integridad de la evidencia original.
2. **Recopilación de evidencias digitales.-** Si mediante los hallazgos del proceso de identificación de incidencias se comprueba que el sistema está comprometido, se requiere establecer la prioridad entre las alternativas de: levantar la operación del sistema o realizar una investigación forense detallada.
3. **Preservación de la evidencia digital.-** será necesario documentar en forma precisa y clara como se ha preservado la evidencia tras su recopilación a lo largo del proceso, es indispensable establecer los métodos adecuados para el almacenamiento y etiquetado de evidencias. Se recomienda la obtención de copias exactas de la evidencia obtenida. Otro factor que debe sustentarse en esta etapa, es el proceso de Cadena de Custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia digital.
4. **Análisis de la evidencia.-** cuyo objetivo primordial es la de reconstruir el acto delictivo, en base a todos los datos disponibles, la línea de tiempo

[30] ***URETA Arreaga, Laura Alexandra;*** Retos a Superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador; *Tesis de Grado Previa a la obtención del Título de. Magister en Sistema de Información Gerencial.*

en que se realizó el ataque, determinando la cadena de acontecimientos desde el instante anterior al inicio del ataque, hasta su descubrimiento.

5. **Documentación y presentación de los resultados.-** se procede con el desarrollo de los informes técnicos o periciales que deberán contener una declaración detallada del análisis realizado, en el cual se debe describir la metodología, las técnicas y los hallazgos encontrados. Es decir, se presentará un Informe Pericial de acuerdo a lo establecido en el Art. 98 del Código de Procedimiento Penal.

Gerberth Adín Ramírez Rivera, expresa “para que todo lo realizado por la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes”.

Las regulaciones que se han establecido en el Ecuador y que están relacionadas con las tecnologías de la información, a más de las ya indicadas en el cuadro anterior, y bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.- Publicada en el Registro Oficial Suplemento # 337 del 18 de mayo del 2004, expedida con la finalidad de llevar a la práctica la disposición constitucional que se señala: “la información es un derecho de las personas que garantiza el Estado”.
La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, en concordancia con el art. 91 y 92 sobre Garantías Jurisdiccionales contempladas en la Constitución Política del Ecuador vigente.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.- La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Reconoce el principio de equivalencia funcional. Se busca que especialmente en los negocios de comercio electrónico las notificaciones sean por medio de correo electrónico, estableciéndose obligatoriedad de notificar por éste medio y por el tradicional para el caso de resoluciones sometidas a Tribunales de Arbitraje. El documento electrónico será considerado como medio de prueba con todos sus efectos legales. Para que existan presunciones legales sobre la veracidad de un documento, éste deberá cumplir los principios de integridad e identidad, para justificar la voluntad contractual de obligarse por dicho documento.

LEY DE PROPIEDAD INTELECTUAL.- nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país. El organismo responsable por la difusión y aplicación de esta Ley es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI).
Esta ley incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software) los cuales son considerados como obras literarias.

LEY DE TELECOMUNICACIONES.- declara que es indispensable proveer a los servicios de telecomunicaciones un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de dichos servicios, y asegurar una adecuada regulación y expansión de los sistemas radioeléctricos,

y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes.

Se ha visto en esta última parte del capítulo lo referente a los de los delitos informáticos y delitos electrónicos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, es importante destacar entonces, que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática.

Ecuador ha dado sus primero pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías; y con la legislación existente los administradores de justicia deben atenerse al verdadero espíritu de la ley y no caer en susceptibilidades de mala interpretación de ley argumentando “que no hay figura delictiva para esta clase de delitos”, reiterando una vez más, que solo estamos ante la presencia de nuevas formas de delinquir, más no ante nuevos delitos.

CAPITULO II
NUEVAS FORMAS DE DELINQUIR EN LA ERA TECNOLÓGICA

2.1. INTRODUCCIÓN

El creciente y significativo avance que ha generado el desarrollo, difusión y uso generalizado de la informática y de las TIC´s y su impacto a nivel mundial, despierta con la explosiva incorporación del Internet, que de modo inexorable está presente en todos los ámbitos del quehacer humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales.

El carácter multifacético de esta novedosa tecnología y su previsible intensidad e impacto en el mediano y largo plazo, ha generado a su vez la creación y proliferación de nuevas formas de delinquir, las que contrastan con el progresivo avance tecnológico en una realidad sociológica y fáctica en permanente transformación.

Así la disciplina del Derecho se halla hoy en una instancia histórica en la que debe responder a estos nuevos y complejos problemas a los que se enfrenta. Por otra parte, la inexistencia de una legislación penal adecuada, posibilita al mismo tiempo, la impunidad y desprotección jurídica de la sociedad en general.

El Derecho Penal, en este sentido, tendrá intervención y legitimación para privar de libertad al agente, solo en cuanto sea respetado el Principio de Legalidad, limitador del poder punitivo Estatal, debiendo previamente ser determinada la acción criminosa como comportamiento ilícito y ser legalmente reprimida a través de legislación penal.

Sabido es, que hoy en día vivimos en la denominada ***"revolución digital",*** caracterizada por el desarrollo de la tecnología en todas sus formas. Esta revolución, que encuentra en Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, en el uso combinado de las computadoras y las redes de comunicación.
Los efectos de la revolución digital o "***era tecnológica",*** se hacen sentir en los distintos sectores de la sociedad: economía, política, educación, etc. Así pues,

la sociedad encontró nuevas formas de interrelacionarse (compras on-line, chats, e-mail, educación a distancia, foros de discusión, transferencias electrónicas, etc.), pero así mismo este fenómeno acarrea consecuencias negativas, ha traído y seguirá trayendo nuevas formas de delinquir, lo que ocasionará cambios profundos a nivel mundial. A partir de la existencia de nuevas formas de operar con la tecnología, aparecen delitos que no son nuevos, sino que existían desde mucho antes de la aparición de la informática, pero que presentan importantes particularidades que han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver, esto debido a que, entre varias otras causas, nuestra legislación tiene muchos vacios legales; y que con el presente trabajo intentaré aportar de alguna manera para una correcta interpretación de la “escasa norma existente” y sus posibles sanciones.

Cualquier persona puede ser o ha sido víctima de tales delitos, que por su nueva forma de cometerse, la falta de una tipificación y de no tener una legislación nacional e internacional adecuada, esta nueva forma de delinquir queda impune.

2.2. EL DELITO INFORMATICO

Todas las actividades humanas que a diario se realizan, como transacciones comerciales y bancarias, comunicación, procesos industriales, las investigaciones, la seguridad, chat, correos electrónicos, etc.; son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Sin embargo, este “desarrollo tecnológico” ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas antes impensadas, ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En esta sociedad informatizada, la mayoría de los quehaceres de nuestra vida cotidiana se encuentra relacionado con la informática, desde su centro laboral, tarjeta de crédito, sus datos personales fichados en los registros y archivos

nacionales, en la actividad tributaria, entre otros; pero como casi todo tiene su lado oscuro, y es en esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías la que debe ser enfrentada por el derecho. Lo que torna de vital importancia el poder identificar y conocer el ambiente y factores que rodean a los delitos informativos, partiendo de una correcta interpretación legal para una adecuada y tipificada sanción penal.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica: **Delitos Informáticos.**

Con estas consideraciones y breve introducción, es necesario definir lo que es Delito Informático, dejando puntualizado que no hay definición universal propia de este delito, sin embargo, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas, destaco entre las más importantes las siguientes:

1. "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material u objeto de la acción criminógena, o como mero símbolo"[31].
2. “Actividades ilícitas que, se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación -la informáticas es el medio o instrumento para realizar el delito-, y que tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos -delitos per se-“[32].
3. María de la Luz Lima, en sentido estricto, el delito Informático “Es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.
4. “Delito informático son actividades ilícitas realizadas por medio de ordenadores o del Internet y/o que tienen como objetivo la destrucción y el daño de ordenadores, medios electrónicos y redes de Internet”[33].

---

[31] ***Sarzana Carlos,*** *obra Criminalitá e tecnología.*
[32] ***Gómez Treviño Joel,*** *Delitos Informáticos; www.joelgomez.com.*
[33] ***http://es.wikipedia.org,*** *Wikipedia Le Enciclopedia Libre: Delitos Informáticos.*

5. El Convenio de Cyber-delincuencia del Consejo de Europa, los define como: “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”.

Cabe destacar y sin establecer una regla genérica, que la computadora constituye un medio para cometer un delito o el objeto sobre el cual recae el mismo, convirtiéndose en el primer supuesto de este tipo de conductas antijurídica. Es por eso, que debe entenderse que el aceptar el uso de la computadora como instrumento delictivo no significa aplicar analogía de ninguna especie, sino adaptar la figura penal a los avances de la técnica. Y ello resulta razonable pues el legislador no puede prever la infinidad de medios a través de los cuales es posible afectar un determinado bien jurídico penalmente protegido.

Pero sin perjuicio de que se enuncien genéricamente una serie de medios, dentro de los cuales tenga cabida el uso de ordenadores, ello no otorgará al delito el carácter de “informático”, un ejemplo de ello: la doble contabilidad llevada por un ordenador con fines de evasión fiscal, la creación de registros falsos con la finalidad de cobrar créditos inexistentes, jubilaciones, estafas etc.

El segundo supuesto que hay que mencionar es el caso en que la informática es el objeto del delito, aspecto de difícil determinación si tomamos en cuenta que se hace necesario diferenciar el hardware del software, y acotar que al primero son generalmente aplicables las normas delictivas tradicionales pues no constituye una nueva forma de propiedad. Distinta situación es el software y de la información almacenada en una computadora, pues los mismos constituyen formas intangibles y su carácter novedoso hace que no siempre hallen cabida en las instituciones tradicionales del derecho.

De esta manera, constituye delito informático cuando se perjudican a datos o programas informáticos, pero no cuando el objeto del daño es un ordenador cuyo resultado, la información que esta contenía queda malograda.

Por lo que se puede inferir que al tipificar un delito informático, lo que se está buscando es tutelar el contenido de la información de un sistema informático, y no el hardware en sí mismo. Se puede hablar también de delito informático en el caso de reproducción ilícita de obras de software de bases de datos o de topografías de semiconductores.

Por último, la situación en la que influyen ambos supuestos, es decir, el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva. El caso más elocuente: destrucción de datos mediante un programa o virus informático. En síntesis, la informática puede constituir un medio o el objeto de una acción típica. En la medida en que se presenten alguno de estos elementos, o ambos, estaremos ante un “delito informático”.

La tipificación o clasificación de los delitos procura, salvaguardar los bienes jurídicos. Estos bienes jurídicos son intereses relevantes de las personas en tantos sujetos sociales, dignos de protección penal frente a conductas que los dañen o pongan en peligro, entonces por ejemplo: con respecto al delito del hurto, el bien jurídico es la propiedad; en caso del delito de homicidio el bien jurídico protegido es la vida; y, en el caso de las nuevas tecnologías el bien jurídico protegido es la información.

Por otra parte, existen diversos tipos de delito informático que pueden ser cometidos y que se encuentran ligados directamente a acciones contra los propios sistemas como son:

- **Acceso no autorizado**: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario. (Violación de la privacidad).
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail:** Lectura de un mensaje electrónico ajeno.
- **Estafas Electrónicas:** A través de compras realizadas haciendo uso de la Internet.

- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes, pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión, ya sea directamente o mediante los llamados "gusanos" o "virus", que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro; pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro.

Las leyes de muchos países no están listas o actualizadas (nuestra legislación está muy corta en este tipo de delitos) para hacer frente al reto derivado de este tipo de delito.

Basta echar un vistazo a nuestra Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos -en adelante, ley 67-, ni siquiera da una definición de este Delito, peor aún tipifica alguna sanción al respecto, dejando por ende en completo estado de indefensión a cualquier persona que sea víctima de este delito tecnológico. De ahí entonces que, claramente puedo interpretar y aplicar el art. 2 del Código Penal que dice: **"[Tipicidad, Vigencia de la ley posterior].- Nadie puede ser reprimido por un acto que no se halle expresamente declarado infracción por la ley penal, ni sufrir una pena que no esté en ella establecida.**

La infracción ha de ser declarada, y la pena establecida, con anterioridad al acto"…

En concordancia con el art. 4 ibídem, que dice: **[Interpretación extensiva e indubio pro reo].- Prohíbase en materia penal la interpretación extensiva. El juez debe atenerse, estrictamente, a la letra de la ley. En los casos de duda se la interpretará en el sentido más favorable al reo.**

Como fácilmente se aprecia, la ley es expresa y clara; si no hay figura delictiva no hay sanción; y en lo referente al delito que nos ocupa, al no existir infracción declarada por la ley, no puede haber sanción, es decir, en nuestra legislación este Delito Informático quedaría en evidente impunidad.

2.3. Los Ciber-Delincuentes: Un Lucrativo Negocio

"Existe una mayor profesionalización en el mundo de la Ciberdelincuencia, al que migran los criminales tradicionales". Raquel C. Pico

La red hace que delinquir sea sencillo y poco complejo, con lo que las posibilidades de obtener una rentabilidad buena de los procesos criminales sean elevadas, al tiempo que, potencia el uso de la red para los delitos tradicionales. En un primer momento las infracciones en el ciberespacio eran cosas de hackers que querían mostrar su poderío, hoy en día es "un modelo más de empresa y más de negocio". Quienes solían comprometer, años atrás, la seguridad de los sistemas informáticos, estaban motivados por el desafío técnico o la curiosidad. Luego apareció el perfil "transgresor" y actualmente se verifican motivaciones delictivas de envergadura, sean de espionaje (industrial o comercial) o robo.

Algunas empresas de antivirus, apuntan que la tendencia de los ciberdelincuentes se orienta hacia la ingeniería social[34] como principal técnica de propagación, su objetivo el robo de información delicada y personal como datos personales y contraseñas.

Con la profesionalización de los **ciberdelincuentes** el **Malware**[35] vive un momento de gran proliferación. Cada pocos minutos aparecen miles de nuevas variedades de amenazas, cuyo fin es fundamentalmente económico. En los últimos tiempos, el phishing no sólo llega a los usuarios a través del e-mail,

---

[34] ***Ingeniería Social.-*** *técnicas diseñadas para persuadir a los usuarios y conseguir información confidencial o para llevar a cabo acciones que suponen la violación de la seguridad de los sistemas de información.*

[35] ***Malware.-*** *ó Software malicioso, programa que se instala en un sistema de información causando daños en ese u otros sistemas o utilizándolos para usos diferentes de los previstos por sus propietarios.*

sino que también puede llegar a través de mensajes en sus teléfonos móviles. Esta nueva tendencia se conoce como vishing.

Muchas veces tuve la inquietud: ¿qué sentido tenía para los ciberdelincuentes crear falsos antivirus e infectar equipos?, con el presente trabajo queda claro cualquier interrogante: **EL DINERO;** y que dicho sea de paso son en cantidades cuantiosas y asombrosas, como se apreciara a continuación, con ciertos ejemplos, estadísticas y referencias.

Panda Security[36] ha elaborado un análisis relacionado con los ciberdelincuentes, explica en detalle el **lucrativo negocio que hay detrás de los falsos antivirus**. Existen unas 200 familias diferentes de falsos antivirus que cada vez son más difíciles de detectar, el estudio también repasa el modelo de negocio implementado, plataformas de distribución, pasarelas de pagos y sistemas de afiliados donde algunos atacantes llegan a ganar miles de dólares en pocos días. Generalmente se les paga por instalación, es decir, infección de otro equipo, y entre un 50 a 90% de comisión por cada venta lograda, nada mal considerando que una licencia de estos falsos programas ronda los 30 a 50 dólares. Esta es sólo una parte del negocio, luego de que el malware está en el equipo las posibilidades de seguir obteniendo beneficios de las víctimas son muchos más[37].

La Ciber-delincuencia se ha convertido en un peligro oculto dentro de nuestra sociedad, y detrás de esta tendencia creciente se encuentra un tipo de malware llamado 'rogueware' o falsos antivirus: y que consiste en falsas soluciones de software diseñadas para robar dinero a los usuarios de ordenadores, cobrándoles por eliminar amenazas que en realidad no existen. Cada mes estas organizaciones generan unos 34 millones de dólares en ganancias

---

[36] ***Panda Security:*** *compañía multinacional de seguridad informática. Sus tecnologías patentadas, llamadas TruPrevent, son un conjunto de capacidades proactivas encaminadas a bloquear virus desconocidos e intrusos. Los productos incluyen: herramientas de seguridad para usuarios domésticos y empresas, protección contra el Cybercrimen y tipos de malware que pueden dañar sistemas de información, como Spam, hackers, spyware, dialers y contenido web no deseado, así como detección de intrusiones en redes WiFi.*

[37] ***Correl Sean Paul-Corrons Luis,*** *El Negocio de los Falsos Antivirus: Análisis del Nuevo Estilo de Fraude Online; PandaLabs Julio 2009.*

gracias a todos los usuarios desprevenidos que, ante el temor del malware en sus equipos, pagan por las licencias de las aplicaciones fraudulentas.

Entre una multitudinaria gama de casos de Ciberdelincuencia, este se llevó a cabo en los Estados Unidos. Un joven fue acusado de "fraude e interferencia de comunicaciones" decidió admitir que había infectado unas 250 mil computadoras para robar los datos personales de sus usuarios y así poder tener acceso a sus respectivas cuentas bancarias. Para lograr su objetivo utilizó mayoritariamente bots[38], programas que se instalan en las PCs y que permiten que se pueda controlar la máquina en forma remota. Se estima que robo unos 1.75 millones de dólares (actualizado a septiembre 2009).

Otro hecho ocurrió en Brasil. Allí, la policía local arrestó a 31 jóvenes estafadores que integraban una red de ciberdelincuentes. Lo que hacían estos muchachos era apoderarse de claves bancarias para transferir el dinero a otras cuentas bancarios o bien directamente para retirar el efectivo. En total, habrían robado unos 343 mil dólares[39] en tres días.

El incremento en el uso de las redes sociales también ha permitido a los ciberdelincuentes hacerse de direcciones y datos para dar más credibilidad a sus "conquistas" y robar al usuario a larga distancia. Esta forma de Ciberdelincuencia opera mediante un correo de alguien que ha visto tu perfil en una red social y quiere conocerte mejor porque le resultaste muy atractivo. Muchos usuarios interesados en conocer al supuesto (a) pretendiente contestan a estas peticiones y comienzan una relación a larga distancia.

En estos correos electrónicos -generalmente de una chica- el o la interesada comenzará a preguntar por sus gustos y luego de intimar con el usuario le contará que está pensando marcharse de su país y le propondrá la posibilidad de irse a vivir al país del que ese usuario sea. Mientras, todos estos emails habrán estado acompañados de diversas fotos de la chica o chico en cuestión.

---

[38] ***Bots:*** *diminutivo de Robot, es un programa informático que realiza funciones muy diversas imitando el comportamiento de un humano. Un bot puede estar diseñado en cualquier lenguaje de programación, funcionar en un servidor o en un cliente, o ser un agente móvil, etc.*

[39] ***Fuente:*** *www.rompecadenas.com, Ciberdelincuentes a la Cárcel.*

Cuando parece que la conquista está a punto de abandonar su país para reunirse con el usuario, ocurre un **"imprevisto de última hora"** -problemas con el visado, sobornos que hay que pagar, pasajes de avión, etc.- y para solucionarlos le pide al usuario una pequeña cantidad de dinero $ 500,00 Ahí comienza el timo, ya que tal conquista no existe, pues es una invención para obtener ese dinero de los usuarios. De acuerdo con PandaLabs si alguno de ellos paga, es probable que la historia se alargue y surjan nuevos problemas que hagan necesario que los usuarios envíen aún más dinero. Según estadísticas de esta empresa, en los 3 primeros meses del 2009 la suma por esta modalidad de Ciber-crimen ascendería a 4 millones de dólares aproximadamente[40].

Otra forma de obtener excelentes beneficios económicos, es mediante las **redes zombis[41] o botnets** son una de las amenazas preferidas por los ciberdelincuentes, se calcula que cada día un cuarto de millón de ordenadores se infecta con algún tipo de troyano que permite controlarlo a distancia.

El tipo de programa malicioso empleado es muy variado. Entre los más frecuentes están los ataques de denegación de servicio, el Spam y phishing. Es un procedimiento de malware muy apetecible para los ciberdelincuentes, hasta el punto de llegar a crear un auténtico mercado del crimen organizado en el que, por ejemplo, el alquiler de una red de bots cuesta 350 euros por semana o 1000 euros al mes. Si además tenemos en cuenta que cada día se infectan 250.000 ordenadores por bots, sobra decir el dinero que se mueve en torno a esta delincuencia y su crecimiento a velocidades de vértigo

Lo único claro en todo esto es que, los usuarios que utilicen las herramientas necesarias para protegerse estarán menos expuestos a las vulnerabilidades, aunque no exentos de ellas.

---

[40] Información tomada de la página web de noticias www.univision.com, con el título ***Ligar en internet puede salir caro,*** *las redes sociales son usadas para timar.*

[41] ***Redes Zombis.-*** *o redes bots, son creadas por un software que se difunde por la red permitiendo controlar un ordenador a distancia sin el conocimiento ni consentimiento del propietario del equipo. El 'zombi' es el ordenador infectado por un bot, mientras que se conoce como 'pastor' al individuo que controla ese bot y establece las órdenes de ejecución.*

2.3.1 Quienes son los Ciber-Delincuentes

Los ciberdelincuentes o criminales informáticos, responden a diferentes tipos de perfiles de individuos o grupos de individuos, que tienen en común un gusto y pasión por las tecnologías y sus posibilidades, y que, aprovechando del desconocimiento de los internautas, diseñan sus estrategias para lograr sus objetivos ilícitos, vulnerando sus derechos y garantías en el uso de las tecnologías de la información

No existe una definición concreta o perfil exacto sobre los ciberdelincuentes. Se habla de características como: solitarios, orientados por las tecnologías y sus avances, inestabilidad emocional y con problemas para definir los límites de sus actuaciones e impactos[42].

"Los ciberdelincuentes o cibercriminales, son grupos delincuenciales organizados y estructurados en células de operación, cuyo objetivo es el empleo de la red como medio de comisión de delitos informáticos"[43].

Los ciberdelincuentes son personas que atacan con software maliciosos con fines económicos de manera ilegal y que pueden tener un área de especialización y estar involucrados en una gran variedad de operaciones comerciales, tales como phishing, troyanos, distribución de Spam, el fraude del clic (clickfraud), desarrollo de malware, etc.[44]

Por lo expuesto, se afirma que son personas que intentan captar a través de mensajes de correo electrónico datos personales o claves de acceso de las posibles víctimas, utilizando tácticas de manipulación para persuadir a los usuarios. Su primer objetivo es que el mensaje parezca real e inspire confianza.

---

[42] ***Acurio del Pino Santiago,*** *Delitos Cibernéticos y Cibercriminalidad.*
[43] ***Acurio del Pino Santiago,*** *Delitos Informáticos y Cibercriminalidad.*
[44] ***cert.inteco.es*** *Software Malicioso: Una Amenaza de Seguridad para la Economía de Internet.*

Los datos personales[45] de los internautas que los ciberdelincuentes obtienen son por ejemplo: números de identificación personal (ID), contraseñas, números de tarjetas, etc., y venden esta información a otros delincuentes que la utilizan para obtener un beneficio financiero. En otros casos, transfieren fondos de todas las cuentas disponibles del cliente, incluyendo tarjetas de crédito, cuentas de ahorro y préstamos sobre el capital de una vivienda, a su cuenta corriente. Luego, utilizan una copia de la tarjeta de crédito o de la tarjeta bancaria del cliente junto con su PIN en cajeros automáticos de todo el mundo para extraer dinero de dicha cuenta.

Para aumentar el número de respuestas los ciberdelincuentes incluyen declaraciones emocionantes o desconcertantes en sus mensajes de correo electrónico. Quieren que las personas reaccionen de manera inmediata y respondan con la información deseada sin pensarlo[46]. Los encabezados más usuales son, entre otras: "***Su cuenta se debe confirmar", "Usuarios del banco advierten", "Actualización de la seguridad de Banco XX"***. Pretextos observados incluyen:

• Necesitan actualizar tu información en sus sistemas

• Medida de seguridad, la información es necesaria como medida de prevención de fraude

• Necesitan confirmar alguna cuenta

• Ocurrió un error en alguna transacción y la información es necesaria para corregirlo

• Ocurrió un error en alguna orden y la información es necesaria para corregirlo, etc.[47].

En definitiva la industria de la Ciberdelincuencia y solo por citar un ejemplo de una infinidad de casos, mueve según estimaciones de una compañía de seguridad en España, 4.130 millones de euros en facturación. Entonces, se

---

[45] ***Datos personales.-*** *aquellos datos o información de carácter personal o íntimo, que son materia de protección en esta ley.* ***(Disposiciones generales, Novena.- Glosario de términos. Ley 67).***

[46] ***www.usbank.com,*** *Fraude por Correo Electrónico: Información y Ayuda.*

[47] ***www.asobancaria.com,*** *Phishing*

pueden obtener beneficios espectaculares partiendo de una inversión relativamente mínima.

De este modo, frente a los 276 millones de dólares que puede costar hacerse con la información privilegiada de las cuentas personales de los internautas, **las mafias virtuales pueden conseguir hasta 5.300 millones de dólares de beneficios**, según la estimación del Informe sobre la Economía Sumergida que ha presentado Symantec.

La Ciber-delincuencia no se encuentra organizada en una o más organizaciones internacionales mafiosas con un capo a la cabeza. Se trata de un mundillo interdependiente que se basa en grupos cuyas operaciones se complementan. Por ejemplo, el individuo o grupo dueño de un botnet (red de ordenadores zombis) capaz de lanzar ataques DDoS[48] o de distribuir mensajes no deseados, necesita dotarse de direcciones de correo. Alguien más, a quien el dueño del boot no necesita conocer ni mantener contacto alguno con él, cumple la función de robar y vender las direcciones necesarias[49].

En términos generales, los modernos ciberdelincuentes tienen que considerar dos técnicas distintas para lograr los resultados finales deseados: distribución e implementación.

Distribución

El primer paso es distribuir e instalar su programa malicioso. Las actuales más conocidas de transmisión de programas maliciosos (también llamadas "vectores de infección") son los mensajes no deseados y los sitios web infectados. El escenario ideal: un ordenador víctima con una vulnerabilidad que permita que un programa malicioso se instale de inmediato, distribuido por un mensaje no deseado o "de paso" mientras se navegaba por Internet. Los

---

[48] ***DDoS: ataque distribuido de denegación de servicio**, (siglas en inglés **D**istributed **D**enial **o**f **S**ervice) el cual se efectúa con la instalación de troyanos en muchas computadoras que pueden estar localizadas en diferentes puntos de todo el mundo.*

[49] *Párrafo tomado de la página web **Viruslist.com: Todo sobre Seguridad en Internet**, La carrera Armamentista en la Ciberdelincuencia.*

creadores de programas maliciosos dependen del robo para la distribución de sus programas y para su supervivencia.

Implementación

Una vez que se distribuye el programa malicioso, el pirata se esforzará por evitar su detección el mayor tiempo posible. Cuanto menos visible sea un programa malicioso ante los sistemas de detección antivirus y ante las respectivas autoridades, mayor será el tiempo que el programa malicioso permitirá el acceso al equipo víctima para recopilar información. Las técnicas más comunes de invisibilidad incluyen las tecnologías rootkit[50], la neutralización de los mensajes de errores detectados en el sistema, los incrementos invisibles del tamaño de los archivos, los numerosos y variados compresores y el bloqueo de los mensajes de advertencia antivirus.

2.3.2. Clases de Ciber-Delincuentes

En la práctica, el término Ciberdelincuencia engloba tres tipos de actividades delictivas:

1. Comprende formas tradicionales de delincuencia, como fraude o falsificación, pero en el contexto cibernético se refiere específicamente a delitos cometidos mediante redes de comunicaciones y sistemas de información electrónicos.
2. Se refiere a la publicación de contenidos ilegales a través de medios de comunicación electrónicos (por ejemplo, imágenes de abuso sexual a menores o incitaciones al odio racial).
3. Incluye delitos específicos de las redes electrónicas, ejemplo: ataques contra sistemas informáticos, denegación de servicio y piratería. Estos ataques también se pueden dirigir contra infraestructuras críticas fundamentales de un país o comunidad y afectar a sistemas de alerta

[50] ***Rootkit.-*** *herramienta que tiene como finalidad esconderse a sí misma y esconder otros programas, archivos, claves de registro, etc., permitiendo al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible*

rápida existentes en numerosos ámbitos, con consecuencias potencialmente desastrosas para el conjunto de la sociedad.

Al hablar de ciberdelincuentes existe un SUJETO ACTIVO ESPECIAL DEL DELITO, y la diferencia única con el delincuente común es que, tienen pericias, ingenios, mañas para el manejo de los sistemas informáticos y se la realiza en el ciberespacio. Las clases de ciberdelincuentes son muy diversos y la diferencia entre sí es la naturaleza de los delitos cometidos. Por ejemplo, para Joel A. Gómez Treviño en su trabajo **"Delitos Informáticos",** habla de una "*Pirámide del Delincuente Informático";* así:

- **TERRORITAS-EXTREMISTAS.-** Usan tecnología y redes informáticas para actividades sociales o políticas ilegales como: actos terroristas (electrónicos o físicos), promover actividades de odio (racistas, homofóbicas, religiosas, etc.) o ilegales (guerrillas, paramilitares, rebeldes, etc.).
- **MERCENARIOS Y TRAFICANTES DE INFORMACIÓN.-** La piratería del software es su más alta arma y suelen ser contratados por empresas de la competencia o ser ex–empleados inconformes de la empresa para dedicarse al Espionaje y Sabotaje Corporativo, además de robo y venta de información de identidad; siendo su objetivo principal el lucro o la venganza.
- **HACKERS, PHREAKS Y CRACKERS.-** Los dos primeros su objetivo es entrar ilícitamente en sistemas informáticos con propósitos de exploración, información o curiosidad; siempre buscan errores en sistemas, sus crímenes aunque ilegales generalmente no intentan causar daño a la información u obtener una ganancia económica**.** El último, su fin causar daño o borrar archivos electrónicos o revelar información confidencial; crean virus y difunden por la red para bloquear o apagar sitios web o páginas de internet con técnicas como la denegación de servicios.

En definitiva son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean y rastrean. Los Hackers posmodernos corsarios de la red, rompen con cierta "facilidad" las encriptadas claves de acceso de los ordenadores más *seguros* del mundo, entran en las redes de información de Gobiernos y organismos oficiales, y simplemente, echan un vistazo y salen dejando una pequeña *tarjeta de visita,* estos piratas no roban, no matan, no destrozan, simplemente observan. Con frecuencia estos ciberdelincuentes usan la "Ingeniería Social", disciplina que ataca al sector más vulnerable de un sistema informático y para el cual no hay solución tecnológica LAS PERSONAS.

Si bien en términos muy generales y muy superficiales en líneas anteriores se indico algo sobre la clase de ciberdelincuentes, es necesario, ahora abordarlos con mayor precisión y objetividad. Se citara a aquellos considerados los más peligros y poderosos, no obstante, de existir una gama infinita de ciberdelincuentes, pero por su importancia y características peculiares se mencionarán solo los siguientes:

HACKERS.- Originariamente, una persona entusiasta de los ordenadores que dedica su tiempo a manejar programas o a crear los suyos propios. Lle gusta husmear por todas partes y llega a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. Son capaces de crear su propio software para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético:

- Toda la información deberá ser libre y gratuita.
- Desconfía de la autoridad. Promueve la descentralización.
- Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza o posición social.

Sin embargo, en la actualidad sus actuaciones se producen en la frontera de lo legal e ilegal; ya que hay una fina línea entre actuar así y producir un daño o

caer en la tentación de robar información. En ciertas legislaciones el mero hecho de colocarse en un sistema ya es delito.

Pero, puedo interpretar diciendo que, el acceso a un sistema, no puede ser considerado a priori como delito, si no se dan los requisitos, objetivos y subjetivos que configuran los tipos penales correspondientes. Sin embargo, la Ley 67 en el ***art. 5.- Confidencialidad y reserva, dice:*** "Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualesquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen esta materia."

En nuestro Código Penal reformado, art 202.1.- ***Delitos contra la información protegida, dice:*** "El que empleando cualquier medio electrónico, informático o afín violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de 6 meses a 1 año y multa de $500,00 a $1.000,00..."

La interpretación de estas normas es simple, es decir, en nuestra legislación, el solo hecho de ingresar a sistemas informáticos sin el consentimiento de su titular, por más curiosidad que tenga esta persona y no le haya causado perjuicio material ni económico, será sancionada conforme se establece en la misma. Ahora bien, el gran problema radica en saber, quien es la "persona" que irrumpió este sistema, donde se encuentra, en que parte lo cometió, estuvo o no dentro de los límites jurisdiccionales aplicables por nuestra ley?.

Problemas y vacios legales que aún quedan por sanar por parte de nuestro legislador.

CRACKER.- Se introducen en sistemas remotos[51] con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar

[51] ***Sistemas Remotos.-*** *o elementos de sistemas, se encuentran físicamente separados de una unidad central. Un puente remoto es un dispositivo que hace posible la comunicación entre, por ejemplo, una LAN y una red de área amplia. Se refiere también al mantenimiento de sistemas a distancia, al acceso*

problemas. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software. Siempre encuentran el modo de romper una protección, pero el problema radica en que esta rotura es difundida a través de la Red para conocimientos de otros.

Crack es sinónimo de rotura y por lo tanto cubre gran parte de la programación de Software y Hardware. Para algunos, se ajusta más al concepto de ciberterrorista, pues su objetivo es romper las defensas de los sistemas informáticos. Si los hackers quieren información como prueba de su habilidad, los crackers la quieren por su valor intrínseco, sea para hacer daño a su legítimo propietario o para obtener beneficios de ella. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en la web como: rutinas desbloqueadoras de claves de acceso o generadores de números para que aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Crean códigos para utilizarlos en la copia de archivos. Sus acciones van desde la destrucción de información a través de virus hasta el robo de datos y venta de ellos. Ejemplo de su actuar ilegal son los millones de CDs con software pirata que circulan por el mundo entero, y muchas personas no llegan a sospechar que parte del soft que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado.

PHREAKERS.- Posee conocimientos profundos y especialista en los sistemas de telefonía terrestres y móviles. En la actualidad poseen conocimientos de tarjetas prepago, pues operan desde cabinas telefónicas o móviles. De esta forma es posible crear clones de tarjetas telefónicas a distancia.

Solo por citar algunas manifestaciones de phreaking se podría distinguir:

a) Call-sell operations: Consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Ha sido aprovechada a nivel internacional por los traficantes de drogas.

---

a aplicaciones residentes en unidades físicamente distantes, etc.; naturalmente, esto implica la utilización de un software especializado.

c) Diverting: penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente.

d) Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio.

EL PIRATA INFORMÁTICO.

Hacen uso del software creado por terceros, a través de copias obtenidas ilegalmente, es decir, sin permiso o licencia del autor, atentando así contra la propiedad intelectual, concretamente violando en primera instancia el art. 1 numeral 2 literal a. de la Ley de Propiedad Intelectual, y enriqueciéndose ilícitamente a más de evadir impuestos. Al software no original se le denomina "copia pirata", en términos reales software robado. En todo el mundo el uso del software ilegal está sujeto a sanciones y penalidades, que se agravan cuando el pirata se convierte en un comercializador de software copiado ilegalmente para lucrar en beneficio propio.

Como se puede apreciar la Ciberdelincuencia no reconoce fronteras, por lo que se hace necesaria una revisión urgente de la legislación nacional y ver si es suficiente para reprimir esta delincuencia informática, cometida por personas vinculadas a empresas e instituciones y por individuos a través de Internet y otras redes.

Nuestra legislación es completamente retrasada y obsoleta respecto de esta clase de delincuencia, la Ley 67 es insuficiente, el Código Penal en sus contados artículos en torno a estos delitos deja ciertos vacios para interpretaciones convencionales. Y el Código de Procedimiento Penal, nada dice respecto del trámite y justamente procedimiento a seguir por la comisión de un delito informático. Justamente por estas razones, innumerables accesos

no autorizados, fraudes informáticos, alteraciones de datos o sabotajes informáticos no son denunciados por temor a la pérdida de la imagen corporativa y además porque nuestras leyes no tipifican sanciones por la comisión de estos delitos.

2.4. La Ciber-Criminalidad

2.4.1. El Sabotaje Informático.- Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Para Marcelo Huerta, "es toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él".

Rodolfo Herrera Bravo, sostiene que "es toda acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional, empleando medios computacionales"[52].

Objetivamente el término sabotaje informático comprende aquellas conductas dirigidas a causar daños en el hardware o software de un sistema. Los métodos utilizados para causar destrozos variados. Básicamente, se puede diferenciar dos grupos:

1. **Conductas dirigidas a causar daños físicos**.- del hardware y software de un sistema, por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico.

---

[52] ***MENESES DIAS, Cristian Andrés,*** *Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno, 30 septiembre 2002.*

2. **Métodos dirigidos a causar daños lógicos**.- es decir, con la técnica informática, o sea, conductas que producen como resultado la destrucción, ocultación, o alteración de datos contenidos en un sistema informático. Este tipo de daño a un sistema se puede alcanzar de diversas formas, por ejemplo: las ***Bombas Lógicas (time bombs)***: la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (2 meses o fecha y hora determinada), o por la aparición de determinada señal, como la presencia de un dato, código o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal. **Virus Informático** programa capaz de multiplicarse por sí mismo y contaminar otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión[53].

2.4.2. Acceso no Autorizado a Servicios Informáticos.- Para los autores chilenos Marcelo Huerta y Claudio Líbano, consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor[54].

Para Claudio Líbano este delito puede clasificarse en: a) hacking directo o acceso indebido, y; b) hacking indirecto o como medio de comisión de otros delitos[55].

Es decir, consiste en la introducción a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ella. A los autores de estas acciones se los conoce como “Hackers”.

---

[53] ***mailxmail.com: Delitos Informáticos, capítulo 9:*** *Tipificación de los Delitos Informáticos.*
[54] ***www.alfa-redi.org:*** *Revista de Derecho Informático, Acceso no autorizado a Sistemas Informáticos*
[55] ***MENESES DIAS, Cristian Andrés,*** *Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno, 30 septiembre 2002.*

Entre los diferentes métodos preferidos se pueden encontrar:

- **Puertas falsas.-** Consiste en aprovechar los accesos que sirven para hacer la revisión o la recuperación de información en caso de errores del sistema.
- **Llave maestra.-** Uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático.
- **Pinchado de líneas.-** Se realiza a través de la interferencia de líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.

Al respecto puedo decir e interpretar según lo descrito que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

2.4.3. El Fraude Informático.- "provecho ilícito que se obtiene con daño patrimonial, mediante el empleo de artificios o engaños idóneos para conducir a otro en error, sirviéndose a su vez de una computadora o vulnerando sus seguridades"[56].

Otros autores opinan que, es "la transferencia no consentida de activos, a través de la introducción o la alteración de datos informatizados, o a través de la manipulación de los programas informáticos de tratamiento de dichos datos".

FORMAS DE FRAUDE:

Manipulación de los datos de entrada.- o sustracción de datos, es el delito informático más común, porque es fácil de cometer y difícil de descubrir. No requiere conocimientos técnicos de informática y puede realizarlo cualquier

[56] ***VALLEJO, María Cristina,*** *Fraude Informático; Revista Judicial, Abogada y Especialista Superior en Derecho Financiero y Bursátil, Ecuador/diciembre 2009.*

persona que tenga acceso a funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Manipulación de programas.- Pasa inadvertida, debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

Manipulación de los datos de salida.- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común, es el fraude a través de los cajeros automáticos; el mismo que se realiza mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Esos fraudes se hacían a base de tarjetas bancarias robadas. Sin embargo, en la actualidad se usa equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito[57].

De ahí entonces que, el fraude puede producirse en cualquiera de las fases de tratamiento o procesamiento informático de datos. Por lo tanto, se puede interpretar que el comportamiento principal de los defraudadores consiste en alterar datos automatizados directamente sustituyendo en el documento unos por otros, o a través, de la modificación del sistema de procesamiento de los mismos. Este delito comprende abusos o interferencias en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención de obtener un provecho y causar un perjuicio económico.

2.4.4. El Espionaje Informático.- Comprende figuras delictivas que atiende al modo operativo que se ejecuta y que puede ser, delitos de *apoderamiento indebido*: de la información; *uso indebido:* usar la información para cualquier fin; y, *conocimiento indebido de la información;* cometidos interfiriendo, interceptando o accediendo al sistema de tratamiento de datos. Y

[57] ***VALLEJO, María Cristina,*** *Fraude Informático; Revista Judicial, Abogada y Especialista Superior en Derecho Financiero y Bursátil, Ecuador/diciembre 2009.*

delitos de *revelación indebida y difusión de datos* cometidos en un sistema de tratamiento de la información[58].

Existen programas de espionaje o spyware; basan su funcionamiento en registrar todo lo que se realiza en un PC, hasta 'clic' en el ratón queda almacenado. Se utiliza para obtener información confidencial. Por ejemplo, una compañía estadounidense, "Lover Spy", ofrece la forma de espiar a la persona deseada enviando una tarjeta postal electrónica, que se duplica en el sistema como un dispositivo oculto, su precio es de 89 dólares, y puede ser instalado hasta en cinco ordenadores. Esta información es posteriormente remitida a la persona que solicitó el servicio de espionaje.

La calificación penal de esta conducta difiere según el tipo de datos a los que se tiene acceso de manera inconsentida o quién sea el sujeto pasivo de la acción delictiva.

2.4.5. El Robo de Servicios.- Dentro de esta categoría se distinguen:

- **Hurto del Tiempo del Ordenador.-** Por ejemplo: uso del Internet, en la cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario para que pueda acceder a dicho servicio, pero el usuario da esa clave a otra persona que no está autorizada para usarlo, causando un perjuicio patrimonial a la empresa proveedora de servicios. Este tipo de conducta se caracteriza por el uso ilegítimo de sistemas informáticos ajenos, usualmente cometido por empleados de sistemas de procesamiento de datos.
- **Apropiación de Informaciones Residuales.**- aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Se llama así porque hay obtención de información a base de rebuscar en restos abandonados por programas o procesos a su terminación. To scavenge, se traduce en recoger basura electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

[58] ***Delitos Informáticos,*** *Contraloría Universitaria; Universidad de Concepción/Julio 2009.*

- **Parasitismo Informático.-** Acceso a internet de forma inalámbrica sin consentimiento o conocimiento del dueño del acceso. Esta conducta suele asociarse a la figura de la Suplantación de personalidad (Impersonation) que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios de servicios informáticos, ej. Uso ilícito de tarjetas de crédito[59].

2.5. Infracciones que no Constituyen Delitos Informáticos.- Se identifican:

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo «mailings electrónicos» al colectivo de usuarios de un 29 Gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate online, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. También se deben tomar en cuenta las obscenidades que se realizan a través de la Internet.

2.6. El Delito Informático y su realidad Procesal en el Ecuador

Las leyes son el reflejo de la realidad social. Este principio rige en todas las normativas del mundo y Ecuador no es la excepción y el denominado “delito informático” es el resultado de nuevas tendencias o medios para delinquir en el país.

Al ser la tipicidad uno de los principios imprescindibles en materia penal es necesario una regulación específica que permita enjuiciar las nuevas formas de delincuencia en un marco adecuado, ya que los “nuevos delitos” no están

[59] ***TINAJEROS ARCE, Erika Patricia,*** Criminalidad Informática en Bolivia; Revista Informática Jurídica, Bolivia 2009.

recogidos en el actual Código Penal, implicando un serio y grave riesgo de caer en la atipicidad, por ende en la impunidad.

Desde mi punto de vista personal, nuestro ordenamiento ha deslindado la legislación específica penal, nuevamente reitero que, siendo el Código Penal el cuerpo legal donde están tipificadas y sanciones las acciones criminales, sin embargo, en torno a esta "nueva modalidad" es absoluta y totalmente vacía. Y los escasos artículos plasmados respecto del delito informático no cubre ni en lo más mínimo las acciones criminales, que dicho sea de paso son infinitas e innumerables, que se desarrollan en el ciberespacio.

No obstante, no debe pensarse que sólo en la norma penal debe establecerse, regularse y determinar lo referente al caso que me ocupa. Existe también en nuestro Derecho la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, pero que lamentablemente es insuficiente. Desde mi punto de vista personal y jurídico, la misma no es contundente peor aun amplia ni objetiva respecto de la nueva realidad tecnológica, y simplemente se limita a determinados aspectos, como Certificados de Firma Electrónica, Entidades de Certificación, etc.¸ que si bien no dejan de ser importantes, de igual manera no menos importantes dejan de ser, por ejemplo: cuando hay delito informático, en qué momento se considera como tal, jurisdicción y competencia, medios de prueba; y en definitiva, todo el proceso y tratamiento, sanciones y tipificaciones que comprende esta nueva era digital.

Para lograr un planteamiento jurídico adaptado al fenómeno constituido por la irrupción de las nuevas tecnologías de la información en la estructura social es que, las mismas no suponen exclusivamente la posibilidad de un conflicto con algún derecho o libertad en concreto, sino que afecta a los pilares básicos de nuestra sociedad puesto que la informática, puede suponer un reto global a una determinada concepción de la sociedad.

Ahora bien, el ordenamiento jurídico, ante la aparición de este fenómeno puede optar entre una de estas dos posturas: o bien regular jurídicamente antes de que los peligros que de tal fenómeno se derivan se materialicen, con el

consiguiente riesgo de que dicha regulación peque de insuficiente como hasta ahora; o bien esperar a que se produzca un más desarrollo del fenómeno en el tiempo, para, de esta forma calibrar y aquilatar mucho mejor la respuesta jurídica y evitar, por tanto, cualquier innecesaria y precipitada intervención legislativa que pudiera entorpecer el desarrollo social y tecnológico.

El progreso tecnológico de la información debe buscar siempre más importantes grados de efectividad pero con el límite constituido por el respeto a los derechos y libertades de los ciudadanos y, en caso de conflicto, optar claramente por la preferencia de estos últimos: al encauzamiento en este sentido del proceso contribuirá decisivamente la existencia de una normativa legal.

Respecto a la realidad y posibilidades de la informática, y el arsenal de medios, técnicas, formas con los que en la actualidad dispone la misma; el ordenamiento jurídico ecuatoriano se muestra claramente insuficiente en relación con la problemática de los Delitos Informáticos. Es necesario, pues, articular una serie de medidas jurídicas que vuelvan a colocar al ciudadano en el papel activo que le corresponde en el Estado de Derecho, medidas que han de dirigirse específicamente a esa nueva realidad que abarca todos los sectores de la estructura social para que los individuos no se vean convertidos en meros objetos de información, sino sujetos que intervienen en los procesos que les afectan.

La fuerza de penetración de la informática en el sector privado es, en la mayoría de los subsectores igual, e incluso superior, a la que se da en el sector estatal. Por todo ello parece evidente la necesidad de una regulación global, lo que, por supuesto, no implica una regulación uniforme. Esta regulación ha de tener en cuenta necesariamente las peculiaridades de los distintos sectores para, de esta forma, hacer frente a los específicos problemas que de cada uno de ellos se derivan.

Pero estas medidas técnicas, administrativas y judiciales deben verse acompañadas del reconocimiento de una serie de derechos de los ciudadanos en relación con la información que les atañe, así como de las correspondientes sanciones penales, previstas para aquellas conductas que supongan una quiebra, ya de las medidas técnicas u organizativas, ya de los derechos reconocidos en esta materia a los ciudadanos.

El recurso al Derecho penal y, por tanto, el carácter grave de las sanciones que puede adoptar y/o plasmar el legislador se halla justificado tanto por la clase de los bienes en juego en esta materia, ya que se trata de garantizar las condiciones necesarias para el ejercicio de la mayor parte de los derechos fundamentales y libertades públicas; como por el carácter también especialmente grave de estas formas de ataque a dichos bienes, ya que colocan al individuo en una situación de absoluta indefensión, pues la mayoría de las veces no llegará ni tan siquiera a conocer que ha sido lesionado en sus derechos, sin saber en la mayoría de los casos quien ocasiono los daños.

La ley ecuatoriana no define el delito informático como tal, lo que sí ha hecho es regular ciertos casos como acceso abusivo a redes y otros delitos relacionados con redes internacionales. Sin perjuicio de que exista o no una definición de que es o que no es un delito informático, el Código Penal y el Código de Procedimiento Penal se debe delimitar, regular y sancionar muchísimos delitos que son susceptibles de ser cometidos en un entorno informático. Y, es allí precisamente, donde el juzgador y los investigadores deben encontrar la relación. Otro aspecto es que, en materia penal se dice que “nadie puede ser juzgado sino por un delito preexistente”, de ahí entonces se podría interpretar que al no estar enunciado todos o los delitos informáticos en general dentro de nuestra legislación, no podría haber sanción; ya que para que exista la misma debe haber regulación previa y exacta de la conducta que se pretende sancionar. Sin embargo, esto no puede ser así, ya que el medio tecnológico, es solo eso Tecnológico, un medio a través del cual se realizan conductas ya tipificadas como delitos. Otro vacio, aunque no es normativo, es

la carencia de medios. Muchas veces existe personal capacitado, certeza del hecho, pero no existen las herramientas para desentrañar la verdad.

La efectiva aplicación de las leyes se complica debido al carácter de Internet, que permite realizar la conducta ilícita en un territorio distinto de aquel en que se produce el daño. Los mecanismos de cooperación internacional para enfrentar la delincuencia informática se presentan como la gran solución frente al delincuente informático.

La delincuencia informática, la criminalidad informática y de las telecomunicaciones, es una realidad que requiere un análisis de múltiples dimensiones para tratar de comprender sus orígenes y así, poder establecer estrategias de prevención y combate de las mismas. Insinuar que la criminalidad informática es un problema jurídico, o tecnológico, o social o de negocio exclusivamente es negarnos la posibilidad de construir un modelo más nutrido de relaciones que busquen profundizar en las problemáticas de las vulnerabilidades, de la inseguridad, de los individuos y sus motivaciones.

CAPITULO III
IMPACTO DE LOS DELITOS INFORMÁTICOS

3.1. Impacto a Nivel General

En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995.

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

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

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Otros delincuentes de la informática pueden sabotear las computadoras para ganarles ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados «gusanos» o

«virus», que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la «cura».

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Bárbara Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

Afirma la Sra. Jenson que una norteamericana fue acechada durante varios años por una persona desconocida que usaba el correo electrónico para amenazar con asesinarla, violar a su hija y exhibir la dirección de su casa en la Internet para que todos la vieran.

Los delincuentes también han utilizado el correo electrónico y los «chat rooms» o salas de tertulia de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos. El Departamento de Justicia de los Estados Unidos dice que se está registrando un incremento de la pedofilia por la Internet.

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

La CyberCop Holding Cell, un servicio de quejas online, hace poco emitió una advertencia sobre un anuncio clasificado de servicio de automóviles que apareció en la Internet. Por un precio fijo de $399, el servicio publicaría una descripción del auto del cliente en una página de la Red y garantizaban que les devolverían el dinero si el vehículo no se vendía en un plazo de 90 días.

Informa CyberCop que varios autos que se habían anunciado en la página electrónica no se vendieron en ese plazo, pero los dueños no pudieron encontrar a ninguno de los autores del servicio clasificado para que les reembolsaran el dinero. Desde entonces, el sitio en la Red de este «servicio» ha sido clausurado.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos de la sociedad en general, cada vez se requieren mayores y mejores conocimientos en las TIC´s. Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentren el eco esperado en los individuos y en las empresas hacia los que va dirigió esta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen esta problemática con el fin de tener un marco legal que se utilice como soporte para el majeo para este tipo de transacciones.

La responsabilidad del Auditor informático no abarca el dar solución al impacto de los delitos informáticos o implementar cambios; su responsabilidad recae en la verificación de controles, evaluación de riesgos, establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan estos delitos.

La concurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que estas se beneficien de todo lo que provee las tecnologías de la información (comunicación remota, interconectividad, comercio electrónico, etc.), al contrario, dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos en caminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc.; y a los profesionales del derecho en la creación, reforma e interpretación de la norma aplicable al caso, si es que ya existe.

La contaminación es de la más variada, entre los últimos ataques a la red y quizá calificar como de los más graves es el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico.

Políticos de algunos países han pedido que se reglamente el uso de la red, de modo que quienes prestan el servicio de Internet registren a los clientes, cuándo y dónde llaman y para qué, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red, protestaran enérgicamente. El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: **Ha abierto la puerta a conductas antisociales y delictivas**.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales[60]. Kevin Mitnik quien con solo 16 años fue un pionero, impuso su lema "La información es pública, es de todos, y nadie tiene derecho a ocultarla" y cuando fue detenido sostuvo que no se creía un delincuente y decía "Un Hacker es solo un curioso, un investigador, y aquí vuestra intención equivale a enviar a un descubridor a la hoguera, como lo hacia la inquisición"

A nivel mundial, en el ámbito de las medianas y grandes empresas, históricamente, la mayor causa de pérdidas de información fue el sabotaje, seguido por los virus informáticos y por último por otras causas como fallas e impericias.

3.2. Impacto a Nivel Social

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

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con

---

[60] ***LEVENE, Ricardo;*** *Delitos y Tecnologías de la Información: Introducción a los Delitos Informáticos, Tipos y Legislación; Noviembre 2008-Argentina.*

conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

También se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

El informe de Evolución de Incidentes de Seguridad que corresponde al año 2007, elaborado anualmente desde 1999 por Red IRIS, determina que el incremento de incidentes que ha habido entre el año 2006 y 2007 es el 63.32% en el que se involucran escaneo de puertos en busca de equipos vulnerables, vulnerabilidades de sistemas web, errores de programación, vulnerabilidades de navegadores más utilizados, ataques de phishing, máquinas zombis, malware y otro tipo de ataques para el cometimiento de fraudes u inhabilitación de servicios, este mismo informe indica que el patrón de ataque continua siendo más dirigido, inteligente y silencioso con algún tipo de trasfondo que puede ser económico, social, religiosos, político o de ansias de poder.

Por último Computer Security Institute (CSI) en conjunto con la Oficina Federal de Investigaciones (FBI), realiza la encuesta anual de Crimen y Seguridad Computarizada, sobre los eventos potencialmente serios y costosos que se han

desarrollado durante el año de la encuesta. En la encuesta se toma información que ha sido prevista por empresas de diferentes sectores como el financiero, legal, educativo, social, servicios de salud, transporte, manufactura, tecnologías de información, entre otros, en los que se analiza en términos de frecuencia, naturaleza y costo que han tenido dichos eventos. Los incidentes ocurridos durante el año 2007, respecto a años anteriores por números de incidentes, se denota un crecimiento de más del 100%, que han sufrido más de 10 ataques. El total de millones de dólares en pérdidas por tipos de ataques fue de $66, 930,950 (194 encuestados) tuvo un incremento del 21 % frente al 2006, en donde se registro una pérdida de $52, 494,290.00 (313 encuestados)[61]

La criminalidad informática organizada ha crecido de manera exponencial, de acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades reportadas y los altos costos que estos involucran para la empresa, los mismos, que son aprovechadas por los intrusos, cabe recalcar dichos intrusos conocen cada vez con más profundidad los detalles de las tecnologías y sus limitaciones, por ello, es cada vez más fácil desaparecer la evidencia y confundir a los investigadores, por lo cual, constituye un reto para los sectores afectados, los legisladores, judiciales, policiales e incluso los especialistas informáticos encargados de su investigación.

El estudio de piratería mundial de software (22), que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares). Las iniciativas dadas para la protección y respeto de las especificaciones de la Ley de Propiedad Intelectual, así como los Derechos de Autor se han desarrollado por campañas de la Business Software Alliance (BSA) tales como “Marca el Límite”, “Anímate 2007”, “Buenos Negocios”, “Evite riesgos, use software legal” como acciones puntuales que impulsan el uso de software legal.

---

61 ***Fuente: CSI-al 2008***

3.3. Impacto en la Esfera Judicial

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se consideren ilegales en el mundo virtual.

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las «computadoras protegidas» -es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia- así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito.

Pese a estos y otros esfuerzos, las autoridades aún afrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos para que se les siga juicio en otro lugar o transferir las pruebas -y a veces los testigos- al lugar donde se cometieron los delitos.

En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada por la doble tipificación penal -la carencia de leyes similares en los dos países que prohibían ese comportamiento- y esto impidió la cooperación oficial, según informa el Departamento de Justicia de los Estados Unidos. Con el tiempo, la

policía del país de los piratas se ofreció a ayudar, pero poco después la piratería terminó, se perdió el rastro y se cerró el caso.

Asimismo, en 1996 el Servicio de Investigación Penal y la Agencia Federal de Investigación (FBI) de los Estados Unidos le siguió la pista a otro pirata hasta un país sudamericano. El pirata informático estaba robando archivos de claves y alterando los registros en computadoras militares, universitarias y otros sistemas privados, muchos de los cuales contenían investigación sobre satélites, radiación e ingeniería energética.

Los oficiales del país sudamericano requisaron el apartamento del pirata e incautaron su equipo de computadora, aduciendo posibles violaciones de las leyes nacionales. Sin embargo, los dos países no habían firmado acuerdos de extradición por delitos de informática sino por delitos de carácter más tradicional. Finalmente se resolvió la situación sólo porque el pirata accedió a negociar su caso, lo que condujo a que se declarara culpable en los Estados Unidos.

Se debe considerar la problemática Jurídica, ya que si bien es ciertos Ecuador ha iniciado los primeros pasos en la generación de Leyes y Decretos que contemplan aspectos significativos de las nuevas tecnologías y también se han establecido penas y 88 sanciones en el Código de Procedimiento Penal, aún se siente la ausencia de legislación, por parte de la sociedad, que sea precisa y coherente, para el tratamiento de esta nueva modalidad de delincuencia, por ello es necesaria la precisión de un marco legal que contemple a los delitos informáticos de una manera integral.

A continuación se detallan bajo este contexto algunos inconvenientes para el manejo de delitos informáticos:

1. Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación: Ministerio Público y Policía Judicial. Las investigaciones a nivel informático en gran parte se dan por denuncias bajo otro contexto de delitos como: robo, daño a la propiedad, estafas, entre otros, que son llevadas por Unidades del Ministerio Público como: la Unidad de Delitos Misceláneos, Unidad de Delitos Financieros y de

Telecomunicaciones, Unidad de Daños contra la Propiedad, debido a la falta de una regulación, o unidad que opere este tipo de infracciones.

2. Falta de especificaciones claras y concisas en la petición de pericias informáticas, pues durante las peticiones de pericias informáticas solicitadas por medio de la autoridad, incurre en términos amplios sobre la "práctica de peritaje informático", en la cual no se especifican requerimientos sólidos sobre lo que se va a investigar, en cuyo caso es importante la comunicación entre los fiscales, jueces y tribunales con los investigadores o peritos de la rama de informática, previo a establecer la diligencia de la pericia.

3. Otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

3.4. Impacto en la Identificación de Delitos a Nivel Mundial

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto.

En el **Manual de las Naciones Unidas** de 1977 se insta a los Estados a que coordinen sus leyes y cooperen en la solución de ese problema. El Grupo de Trabajo Europeo sobre delitos en la tecnología de la informática ha publicado un Manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

El Instituto Europeo de Investigación Antivirus colabora con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las

computadoras o «caballos de Troya». También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

En 1997, los países del Grupo de los Ocho aprobaron una estrategia innovadora en la guerra contra el delito de «tecnología de punta». El Grupo acordó que establecería modos de determinar rápidamente la proveniencia de los ataques por computadora e identificar a los piratas, usar enlaces por vídeo para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.

El Grupo de los Ocho ha dispuesto ahora centros de coordinación abiertos 24 horas al día, siete días a la semana para los encargados de hacer cumplir la ley. Estos centros apoyan las investigaciones de otros Estados mediante el suministro de información vital o ayuda en asuntos jurídicos, tales como entrevistas a testigos o recolección de pruebas consistentes en datos electrónicos.

Un obstáculo mayor opuesto a la adopción de una estrategia del tipo Grupo de los Ocho a nivel internacional es que algunos países no tienen la experiencia técnica ni las leyes que permitirían a los agentes actuar con rapidez en la búsqueda de pruebas en sitios electrónicos -antes de que se pierdan- o transferirlas al lugar donde se esté enjuiciando a los infractores.

A manera de referencias, por ejemplo, cito algunas consideraciones importantes respecto de este delito a nivel mundial.

En España, la Ley no condena el mero acceso y permanencia no autorizada en un sistema informático, lo que se conoce como **hacking directo**. En cuanto a los **virus**, la legislación española tampoco penaliza a sus creadores, solamente a aquellos que los emplean con fines maliciosos. Sí tiene una repercusión a efectos penales importantes, el atentado a la propiedad intelectual (copia de software), distribuir ilegalmente copias de productos con derechos de autor a través de la Red, como los programas p2p (de amigo a amigo), así como la

tenencia y distribución de programas orientados a la supresión de los mecanismos de protección contra la copia de dichos productos.

En su vigente Código Penal no se halla un título específico que contenga los delitos informáticos. En su articulado, se encuentran diseminados multitud de tipos penales cuya comisión cabría dentro del concepto amplio de delito informático. Tal es el caso de la apología del terrorismo a través de Internet, o el blanqueo de capitales[62].

El mayor consenso, hasta la fecha sobre la identificación de los delitos informáticos, lo ofrece el Convenio de Ciberdelincuencia del Consejo de Europa, firmado por los países participantes el 23 de noviembre del 2001 en Budapest, pero solo ratificado por ocho países. En este Convenio se acotan los delitos informáticos en cuatro grupos y se definen los tipos penales que han de considerarse como delito informático. Estos son:

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.**

Acceso ilícito a sistemas informáticos.

Interceptación ilícita de datos informáticos.

Interferencia en el funcionamiento de un sistema informático.

Abuso de dispositivos que faciliten la comisión de los anteriores delitos.

2. **Delitos informáticos.**

Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

---

[62] ***www.tuabogadodefensor.com Delitos Informáticos y Tecnológicos:*** *Los Delitos Informáticos en el Código Penal Español.*

3. **Delitos relacionados con el contenido.**

Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de contenidos de pornografía infantil.

4. **Delitos relacionados con infracciones a la propiedad intelectual y derechos afines.**

Posteriormente, el 28 de Enero del 2003, se promulgó a la firma un Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos[63].

Es de destacar que conductas tan frecuentes en esta Sociedad de la Información, como el Spam, difícilmente encuentran cabida entre los delitos tipificados en nuestro Código Penal, por lo que no son perseguibles por vía penal.

Apoyándose también en la negligencia de los usuarios, los autores de virus emplean la Ingeniería Social para que sus creaciones se propaguen rápidamente, para ello atraen la atención del usuario y consiguen que realicen alguna acción, que normalmente consiste en abrir un fichero que es el "regalito" del atacante. Ejemplos paradigmáticos de estos ganchos serían los virus **I love You y Kournikova, Pokemon, Pikachu, y las diferentes versiones del W32 (**que utiliza las listas de e-mails de las víctimas) **y el troyano Butano, Nesky**[64].

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

La CyberCop Holding Cell, un servicio de quejas online, hace poco emitió una advertencia sobre un anuncio clasificado de servicio de automóviles que

[63] ***Fuente:*** *Dirección General de la Guardia Civil-Grupo de Delitos Telemáticos.*
[64] ***www.tuabogadodefensor.com Comunicado de Prensa:*** *Lucha contra la Delincuencia en Internet, Abril 2008.*

apareció en la Internet. Por un precio fijo de $399, el servicio publicaría una descripción del auto del cliente en una página de la Red y garantizaban que les devolverían el dinero si el vehículo no se vendía en un plazo de 90 días.
Delitos informáticos cuestan un billón de dólares a nivel mundial. Según un estudio de McAfee, la mayor parte de ese dinero representa la pérdida de información y propiedad intelectual, así como la reparación de los daños ocasionados[65].

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

La mejor estrategia contra los asaltantes no es la tecnología, es la formación de los usuarios, ya que si estamos conscientes de la posibilidad de ataques y que éstos serán contra nuestros propios intereses, asumiremos la función de guardianes del sistema.

[65] ***Fuente: eltiempo.com;*** *febrero 2009.*

CAPITULO IV

SEGURIDAD CONTRA LOS DELITOS INFORMÁTICOS

La importancia creciente de las infraestructuras de información y comunicación abre nuevos caminos a conductas delictivas. Esta es la razón por la que hay que adoptar medidas para luchar contra el contenido ilícito y perjudicial en Internet con el fin de proteger los derechos de la propiedad intelectual y los datos de carácter personal, promover el comercio electrónico y reforzar la seguridad en las transacciones; y en general todo lo que se realiza en este "mágico mundo cibernético".

Los riesgos que se pueden devengar de los insuficientes controles están muy relacionados con la mayor exposición de información sensitiva, nuevas tecnologías sin controles apropiados, autorizaciones electrónicas, concentración de funciones, integridad de datos, escasez de herramientas de auditorías y en general de la Sociedad de la Información o TIC´s. La Seguridad Informática, aunque es responsabilidad de todas las personas capaces de afectar la seguridad de datos y de los sistemas computarizados, existen funciones muy específicas que se encuentran directamente involucradas con esta parte, ellas son: la gerencia, el responsable del plan de seguridad, los responsables funcionales y autores de las aplicaciones, los administradores de los sistemas y en última instancia los usuarios de los sistemas. Además ha de tenerse en cuenta la manutención adecuada de costo-beneficio.

Toda entidad y usuarios particulares que emplean sistemas informáticos para el control de su gestión deben implementar un plan de seguridad informática óptimo y eficaz, y un plan de contingencia que garantiza la adecuada función de estos, tanto físicos como lógicos. Estos programas permitirán asegurar la existencia de una seguridad apropiada y un costo efectivo para cada sistema de aplicación que se encuentre en explotación; programa que incluye los controles a implementar, adquisición e instalación de tecnología de apoyo a las medidas de seguridad, administración de la seguridad informática, evaluación de las vulnerabilidades y debilidades de los sistemas y soluciones a los problemas de seguridad. Solo a manera de referencia en el 2006, IDC

Research realizó una encuesta en donde el 90% de los usuarios expresó gran interés sobre la seguridad del Internet, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la Red.

Realizar actividades delictivas a través de Internet requiere unos conocimientos técnicos sofisticados que no están al alcance de cualquiera.

Las posibilidades de protección de las comunicaciones electrónicas existen. Hay programas de ordenador gratuitos y fáciles de usar que permiten a cualquier usuario la encriptación de sus mensajes de forma que queda garantizado que sólo el destinatario podrá entenderlos. Los certificados y firmas electrónicas garantizan la identidad de los sujetos con mucha mayor garantía que cualquier fedatario tradicional. Los sistemas de almacenamiento de datos y su protección frente a accidentes fortuitos o ataques intencionados son más fáciles, baratos y seguros que las cajas fuertes o cámaras de seguridad. Lo que ocurre es que no hay una "cultura" de la seguridad en Internet[66].

La protección legal del comercio electrónico ha requerido la elaboración o creación de nuevas normas. El reconocimiento jurídico de las firmas electrónicas y del arbitraje electrónico debe establecer un marco legal que garantice la calidad de los certificados y agilizar los trámites judiciales. Los gobiernos de todo el mundo están interesados en promover el desarrollo del comercio electrónico por lo que están impulsando reformas legales y fiscales que permiten y agilicen las transacciones a través de Internet.

La seguridad en Internet y las leyes que la protegen, están basadas principalmente en los sistemas de encriptación. Esos sistemas son los que permiten que las informaciones que circulan por Internet sean indescifrables, ininteligibles, para cualquier persona que no sea aquella a la que va destinada.

[66] ***www.eumed.net*** Seguridad en Internet

4.1. Seguridad en Internet

Intentar comunicar un secreto o cualquier tipo de información en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto, información o actividad de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Sin embargo, la **Seguridad en Internet** no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet dicha privacidad no desaparece. La privacidad además de confidencialidad incluye anonimato[67].

Hay realmente varias partes de la seguridad que confunden. La Seguridad significa guardar **"Algo Seguro";** Algo puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactiva., **"Seguro"** los medios son protegidos desde el acceso, el uso o alteración no autorizada. Para guardar objetos seguros, es necesario lo siguiente:

- ✓ **Autenticación** (promesa de identidad), es decir, la prevención de suplantaciones, para garantizar que quien firma un mensaje es realmente quien dice ser.
- ✓ **Autorización** dar permiso a una o varias personas de poder realizar ciertas funciones, negando esta posibilidad a otras sancionándolas si las realizan).
- ✓ **Privacidad o confidencialidad**, referente a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio puede ser interceptada y copiada: las líneas «pinchadas» la intercepción o

[67] ***es.wikipedia.com*** Seguridad en Internet.

recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

- ✓ **La integridad de datos** se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen.
- ✓ **Disponibilidad de la información,** seguridad a que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- ✓ **No rechazo** (protección contra alguien que niega que ellos originaron la comunicación o datos).
- ✓ **Controles de acceso,** quien tiene o no autorización para acceder a una pieza de información determinada.

Son los requerimientos básicos para la seguridad y que variaran ligeramente dependiendo de lo que se está asegurado.

Actualmente dicha seguridad es atacada por:

Uso de password, Uso de Vulnerabilidades conocidas, Uso de brechas en protocolos.

Examen de fuentes para descubrir nuevas brechas, Empleo de ataque ICMP[68].

Abuso de FTP (File Transfer Protocol), Empleo de programas "Sniffers[69]", Spoofing[70] de dirección IP fuente.

Los valores que se protegen son:

---

[68] *El **Protocolo de Mensajes de Control de Internet** o **ICMP** (por sus siglas de **I**nternet **C**ontrol **M**essage **P**rotocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado*

[69] *un **packet sniffer** es un programa de captura de las tramas de red, es decir, que el medio de transmisión sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.*

[70] ***Spoofing.-** en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.*

Hardware: tarjetas, teclados, terminales, impresoras, servidores de terminales.

Software: programas fuente, utilitarios, programas de diagnóstico, sistemas operativos, programas de comunicación.

Datos: durante la ejecución, almacenados, resultados de auditoría, bases de datos, en tránsito sobre medios de comunicación.

Personas: usuarios, empleados que operan en los sistemas

Documentación: manuales de programas, hardware, sistemas, procedimientos locales de administración, reglamento.

Por otro lado, y para comprender los tipos de amenazas a la seguridad que existen, daré a conocer los requisitos de seguridad en computadores y redes que implica tres exigencias:

- **Secreto:** que la información en una computadora sea accesible para lectura sólo a usuarios autorizados, acceso que incluye la impresión, mostrar en pantalla y otras formas que incluyan cualquier método de dar a conocer la existencia de un objeto.
- **Integridad:** que los recursos de un computador sean modificados solo por usuarios autorizados, modificación que incluye escribir, cambiar de estado, suprimir y crear.
- **Disponibilidad:** recursos del computador estén disponibles a usuarios autorizados[71].

Se han considerado e identificado como posibles amenazas o agresiones:

ATAQUES PASIVOS.- Estas agresiones son el tipo de las escuchas o monitorizaciones ocultas de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de estas agresiones:

[71] ***www.wikipedia.com*** *Requisitos y Amenazas de la Seguridad*

1. **Divulgación del Contenido de un Mensaje.-** Sencillo, una conversación telefónica, mensaje de correo electrónico o un fichero transferido pueden contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.
2. **Análisis del Tráfico.**- Para entender, supongamos que hay un medio de enmascarar (técnica de cifrado) el contenido de los mensajes u otra información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados.

ATAQUES ACTIVOS

Estas agresiones suponen la modificación del flujo de datos o la creación de flujos falsos y se subdivide en 4 categorías, a saber

1. **Enmascaramiento.-** se da cuando una entidad pretende ser otra entidad diferente. Por ejemplo, se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.
2. **Repetición** captura pasiva de unidades de datos y su retransmisión subsiguiente para producir un efecto no autorizado.
3. **Modificación de mensajes** significa que alguna porción de un mensaje legítimo se altera o que se retrasa o se reordena para producir un efecto no autorizado.
4. **Denegación de un servicio** impide o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o

sobrecargándola con mensajes de forma que se degrade su rendimiento.

Una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es difícil prevenir una agresión activa, pues para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación.

Existen mecanismos para evitar o por lo menos controlar estas agresiones, una de ellas es el Monitoreo de Red, entendido como "**el uso de sistemas que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager[72] u otras alarmas"**. Aquí se realiza un examen de los "ficheros log[73]" que producen y guardan la mayoría de los sistemas de manera regular, primera línea de defensa. Por otro lado, está la utilización de herramientas de los sistemas operativos para constituir herramientas propias tales como: elecklists de usuarios, permisos, propiedades de files. Además se deben efectuar constantes variaciones en el calendario y cronograma del monitoreo, ya que cuando la administración del sistema ejecuta diferentes acciones de monitoreo en diversos momentos del día es más difícil para los intrusos predecir las acciones de la administración y mantenerse encubiertos. Sin embargo, monitorear no es suficiente para garantizar que su sistema sea seguro pues se puede monitorizar todo el tráfico que se mueve a través del conmutador.

Por el medio utilizado para la difusión de este delito donde Internet es el instrumento de difusión, tan difícil es detectar el delito como probarlo. El elemento probatorio como en todos los delitos que se cometen es la base de su juzgar y por ende de su sanción. Esta búsqueda se torna mucho más compleja por el medio que se utiliza para ello y por las características del mismo; ya que no existe forma de determinar fehacientemente cuál era el estado anterior de

---

[72] ***Pager.-*** *dispositivo de telecomunicaciones simple que recibe mensajes de texto corto, ej. Beeaper.*
[73] ***Ficheros Log.-*** *son grabaciones de la actividad del sitio web a lo largo de un periodo de tiempo en particular. Esta información incluye las peticiones de cada página desglosadas por fecha y hora del día, la dirección IP de los visitantes, sitios desde los que llegaron los visitantes, etc.*

los datos, puesto que la información en estado digital es adulterable, y la simple auditoría contable o financiera común pierde su eficacia ante este nuevo tipo de figura delictiva. Inclusive a manera de referencia, la sanción puede llegar hasta ser compleja su determinación, partiendo de que por ejemplo en el caso de la responsabilidad civil sería difícil determinar el valor que dicha información tenía, debido a que el valor de la misma es subjetiva. La complejidad de su determinación se incrementa si tenemos en cuenta que los medios empleados son sólo conocidos por especialistas, que el autor de la conducta antijurídica tiene la facilidad de borrar las huellas o rastros de identificación, y el tiempo que puede mediar entre la acción y el efecto.

En la actualidad nuestro ordenamiento penal deja desprotegido aparentemente a la víctima de los ataques de delincuentes informáticos por no recoger en su articulado normas específicas que tipifiquen cada una de los casos que pudieran darse. Nuestros tribunales por su parte con todas las intenciones de impartir justicia tienen en cuenta estas actividades delictivas atendiendo a la acción del comisor y los resultados que esta provoca, asemejándola a aquella que está recogida en el Código Penal. Siendo así entendida una violación del correo electrónico que ataca la intimidad del usuario como una mera violación de la correspondencia pues el bien jurídico que se daña será en ambos casos la información. En este supuesto la acción del comisor será apropiarse o tener conocimiento del contenido del texto que por cualquiera de ambas vías se envía, sin el consentimiento previo de su destinatario, y mucho menos sin una autorización legal que fundamente estos actos en el caso de que el transgresor de esta norma fuera una persona jurídica que actúe mediante acuerdo de los socios o en representación de la misma en buscas de pruebas que demuestren que el destinatario utiliza la red para cometer posteriores delitos que atacan la propiedad de dicha entidad[74].

Actualmente la auditoria informática definida como el conjunto de técnicas y procedimientos destinados a la evaluación y control de los Sistemas Informáticos entendidos estos en su amplia acepción ; es la encargada del

[74] ***ARREGOITIA LOPEZ, Siura Laura;*** *Protección contra los Delitos Informáticos en cuba;* ***Facultad de Derecho. Universidad de La Habana***

cumplimiento de los controles internos de las entidades que utilicen en nuestro país sistemas de este tipo; despliega por esto la función de revisión en un ciclo: administración de la seguridad de la red, seguridad de las comunicaciones, seguridad de las aplicaciones y seguridad física.

Técnicamente este sistema de protección tecnológica debe estar aparejado al establecimiento de las normas penales pertinentes que se ajusten al nuevo problema en nuestro caso particular como nación, donde ya se han registrado casos delictivos de esta índole. La ley penal como última ratio podrá dar frente a las situaciones que se ventilen ante el incumplimiento de los reglamentos internos de las entidades, sancionando las acciones negativas que se produzcan.

Podemos apreciar que la legislación informática hace referencia a los rasgos característicos de este programa de seguridad informática, tales como: integridad, confidencialidad y disponibilidad de la información. La Seguridad Informática además de ser el bien jurídico tutelado, puede conceptualizarse como la operación de los sistemas de información, rigiéndose por las características que las distingue anteriormente mencionadas, tenemos que la información debe ser fidedigna y completa, nadie que no sea el usuario tiene derecho a cambiarla; que el usuario debe tener la información en el momento que la necesite; y sin su consentimiento nadie debe tener acceso y menos a divulgarla. A estas características principales por las que se distingue, le acompañan otras dos: la consistencia, mediante la cual el sistema debe comportarse siempre igual aun después de un cambio; la de control de usuario teniéndose aquí el control sobre quién entra al sistema y qué hace. Por otro lado, constituye el núcleo del control interno, y su principal objetivo es documentar las directivas o decisiones generales referentes a la seguridad de los sistemas, estableciendo las metas a alcanzar y asignando las responsabilidades.

4.2. Firma Electrónica

Hoy en día, la firma electrónica cumple un papel muy importante respecto al déficit de seguridad que existe en la "Red de Redes", puesto que su "utilización puede *garantizar la integridad del mensaje, su reconocimiento y su autenticación;* es decir, es el procedimiento por el cual se asegura la identidad del remitente del mensaje". El comercio en Internet, está ligado íntimamente con la firma electrónica, debido a que para realizar transacciones comerciales, necesita su firma para que el documento tenga validez.

El acceso a las redes públicas, unido a la seguridad reinante en las redes privadas, hace que Internet, necesite de una serie de mecanismos que generen seguridad. La FIRMA ELECTRONICA aparece como una respuesta a esta deficiencia, que a su vez se manifiesta en la necesidad de confiabilidad, integridad, identidad y no repudio en las comunicaciones. La deficiencia significa que, cuando se establece una comunicación y uno de los interlocutores transfiere información al segundo, no se asegura que el mensaje enviado sea recibido únicamente por el destinatario pretendido (Confidencialidad); además es posible que la información sea alterada por un agente distinto del emisor a lo largo de su recorrido, antes de ser recibida por su destinatario (Integridad); y además, ninguno de los agentes en la comunicación puede cerciorarse de la identidad del otro, pudiendo no ser éste otro quien dice ser; y finalmente, puede que el usuario origen de una comunicación se retracte de su autoría, e impida con ello garantizar el no repudio"[75].

En nuestro contexto territorial, El Consejo Nacional de Telecomunicaciones (CONATEL) como organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados en el Ecuador, es el encargado de acreditar y registrar a estas entidades, previo el cumplimiento de requisitos de carácter técnico, legal y financiero que permitan demostrar la capacidad de operación y solvencia de las mismas. Para ello, el

[75] ***DOMÍNGUEZ GRAGERA, María Luisa.-*** Normativa Aplicable a la Firma Electrónica (Directiva 99/93) Comercio Electrónico y Real Decreto- Ley 14/1999. Editorial La Ley. España. 2002. pp. 1339.

Regulador realizó importantes cambios normativos que permita superar los obstáculos respecto al derecho de confidencialidad y Seguridad en la Información, y acreditó al Banco Central del Ecuador como la primera Entidad de Certificación de Información y Servicios relacionados en el país, por lo que corresponderá a esta entidad dar la seguridad y confiabilidad en las transacciones en las que se utilice la firma electrónica.

La firma electrónica no tiene relación alguna con el escaneo o digitalización de la firma autógrafa tradicional, sino que consiste en una combinación de algoritmos de encriptación que mediante el uso de una clave pública y privada permiten cifrar y descifrar la información. Cada firma electrónica está vinculada a un certificado electrónico el cual garantiza la identidad y autoría del firmante, así la seguridad, confidencialidad, integridad y transparencia en los procesos electrónicos son mayores que en los procesos físicos y el ahorro de tiempo y recursos genera beneficios tangibles a corto y mediano plazo.

Firma Electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos"[76]

Las Entidades de Certificación de Información y Servicios Relacionados son las encargadas de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como de la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de la infraestructura pertinente y el recurso humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad.

Entidades de Certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el

[76] ***Art. 13 CAPÍTULO I DE LAS FIRMAS ELECTRÓNICAS;*** *Ley de Comercio electrónico, Firmas Electrónicas y Mensajes de Datos, actualizada a agosto de 2007.*

Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y reglamento que deberá expedir el Presidente de la República"[77].

Así mismo, dentro de los cambios normativos realizados se han previsto mecanismos para precautelar la disponibilidad en la prestación de servicios de certificación de información y de esta forma garantizar los derechos de los usuarios. Además la Secretaría Nacional de Telecomunicaciones –SENATEL- en alianza con sectores públicos y privados estratégicos, se encuentra coordinando planes y acciones para difusión, uso y masificación de una cultura electrónica y telemática a nivel nacional mediante el uso y aplicación de herramientas tecnológicas actuales como la firma electrónica.[78]

Ahora bien, profundizando un poco más sobre esta "Firma Electrónica", daré a conocer muchos de sus aspectos y característica, funcionamiento y creación, así como el valor jurídico de la misma, y unas cuantas consideraciones más que a continuación detallo.

El problema fundamental que plantean las transacciones a través de Internet desde el punto de vista jurídico, se puede resumir en cuatro temas y que deben tomarse en cuenta para que la información no sea alterada por ningún concepto y son:

1. CONFIDENCIALIDAD, secreto de la información contenida en el mensaje.
2. INTEGRIDAD, de la información no pueda ser manipulada en el proceso de envío.
3. AUTENTICIDAD, que la información sea enviada por quien aparece como emisor y recibida por aquel a quien va dirigida.
4. NO REPUDIO, asegura que no se pueda negar la autoría del mensaje enviado.

---

[77] ***Art. 29 CAPÍTULO III, DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN,*** *Ley de comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, actualizada a agosto 2007.*

[78] **www.conatel.gov.ec;** La Certificación de Información de la firma electrónica cuenta con regulación del CONATEL

Para garantizar el cumplimiento de estos requisitos, se plantearon dos alternativas:

1.- CRIPTOGRAFIA[79] SIMETRICA, obliga a los interlocutores a utilizar la misma clave para encriptar y desencriptar el mensaje[80].

2.- CRIPTOGRAFIA ASIMETRICA, consisten en la asignación de dos claves, una pública y otra privada, asociadas a un solo interlocutor. Así, la clave privada es conocida únicamente por su propietario, y con esa clave firma electrónicamente un documento; y la clave pública es conocida por todos para que el destinatario abra el documento.

Este sistema parece el más adecuado y utilizado en la práctica para el cumplimiento de los requisitos anteriores, bajo la denominación RSA[81], contemplado en el documento de la ISO 7498-2, de Julio de 1988, que señala la arquitectura de seguridad para proteger las comunicaciones de los usuarios de las redes.

En definitiva este sistema es conocido como PKI, que es una plataforma de seguridad que permite a los usuarios autorizados ingresar y operar en el Portal de Servicios Electrónicos, mediante una firma electrónica de clave pública y privada basado en un par de llaves asimétricas, y que están íntimamente vinculadas a la Entidad Certificadora (BCE) como una tercera parte confiable que certifica y autentica las transacciones electrónicas, realizando servicios tales como: **Certificación y Revocación de Claves, Consultas de directorio seguro, Emisión de certificados, etc.**

---

[79] ***CRIPTOGRAFÍA.-*** *del griego krypto, «oculto», y graphos, «escribir», «escritura oculta») es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales, se emplea para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Protege la información de modificaciones y utilización no autorizada. Maneja algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro extremo.*

[80] *Esta técnica fue desarrollada por IBM, pero fracasó por su inseguridad en el secreto y confidencialidad de dicha clave.*

[81] ***RSA.-*** *Es un sistema criptográfico de clave pública. Un algoritmo para cifrar, los mensajes enviados se representan mediante números. (Rivest, Shamir y Adelman).*

Desde un punto de vista técnico, se puede decir que de este sistema asimétrico nace la Firma Electrónica que se basan fundamentalmente en principios criptográficos, en algoritmos matemáticos que aplicados a los textos le darán la confidencialidad necesaria y la seguridad de que el mismo no ha sido modificado.

Para beneficiarnos de las ventajas que nos brinda la firma electrónica, siempre deberemos como ya se ha dicho acudir a una Entidad Certificadora él mismo garantizará nuestra identificación personal. Una vez identificados, generará nuestras claves (pública y privada) así como el programa necesario para su uso que deberá instalarse en nuestro ordenador personal. Deberemos custodiar nuestra clave privada que residirá en la CPU de nuestro ordenador o estará incorporada en tarjeta inteligente.

Las tecnologías de autenticación han experimentado un importante avance en los últimos años, debido a la necesidad de proteger las comunicaciones en redes abiertas como Internet y brindar una imperiosa necesidad de seguridad, debido a vulnerabilidades de acceso a comunicaciones e información de la cual es susceptible la “Red de Redes”. De ahí entonces que la autenticación es un servicio de seguridad que tiene por objeto corroborar la identidad alegada por un usuario participante en una “Sesión”.

La mayoría de las regulaciones sobre autenticación han adoptado el concepto de firma electrónica, que es un concepto más genérico y tecnológicamente neutral, que conceptos como el de firma digital. Siendo la primera el GENERO y la segunda la ESPECIE.
Indica Ribargorda[82], existen tres procedimientos habituales para lograr la autenticación:

1. Un dato exclusivamente conocido por el usuario: **contraseña** o **password**.
2. Un objeto en poder del usuario: una tarjeta de banda magnética o chip.

---

[82] *El aporte del autor recoge la categorización realizada en las normas técnicas de autenticación, en especial los trabajos de la ISO.*

3. Un procedimiento biométrico: **huella dactilar, geometría de la mano, iris del ojo**.

No todas las tecnologías de autenticación ofrecen las mismas garantías al usuario, y por este motivo, también la regulación jurídica normalmente distingue entre diferentes niveles de firma electrónica, con diferentes efectos jurídicos. En este punto, daré a conocer los niveles de firma electrónica existentes en la Directiva 99/93 del 13 de Diciembre[83], y que me permito detallar a continuación:

- **FIRMA ELECTRÓNICA ORDINARIA.-** son datos en forma electrónica anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medios de autenticación". Con esta definición se puede interpretar que, permite que todos los mecanismos técnicos de autenticación sean potencialmente considerados como la firma electrónica de una persona.

  Un modelo de esta firma y por los mecanismos de autenticación es un PIN y de hecho, en gran cantidad de contratos de acceso a servicios telemáticos, se establece que el PIN del usuario es la firma electrónica del usuario. A pesar de que esta consideración es correcta, la interpretación puede ser diferente, pues la realidad es que el PIN, al igual que los mecanismos de seguridad simétricos, en los que ambas partes conocen los datos para la autenticación, puede utilizarse para lograr una autenticación PERSONAL, y difícilmente va a permitir una autenticación en el vincular UN MENSAJE DE DATOS CON ESA PERSONA.

  A pesar de calificarse al PIN como firma electrónica ordinaria, la razón y sentido común indica que no puede ser en todos los casos **Equivalente** a una firma manuscrita, porque no establece un vínculo con el firmante.

- **FIRMA ELECTRÓNICA AVANZADA.-** Aquella firma que está vinculada al firmante de manera única permitiendo la identificación del mismo; y ha

[83] ***I CONGRESO MUNDIAL DE INFORMÁTICA Y DERECHO***, *Tipología Legal de la Firma Electrónica.*

sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; estando vinculada a los datos a los que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable[84].

De esta definición se desprende que, esta firma necesita estar vinculada entre el mensaje firmado y el poseedor de la clave privada de firma: que será un dispositivo o aplicación informática operada por una persona física o jurídica; es un mecanismo de identificación real del firmante; control exclusivo de creación de la firma; y, estar vinculada con los datos firmados.

Esta firma tiene en relación con el documento electrónico, el mismo valor jurídico que la firma manuscrita en el documento papel. Será admitida como prueba en juicio y valorada conforme a los criterios de apreciación judicial establecidos en las normas procesales. El documento firmado electrónicamente no tiene valor de documento público: la firma electrónica no sustituye la función del fedatario público respecto de la formalización, validez y eficacia de las obligaciones y los contratos[85].

De lo dicho, se dice que sólo una firma digital puede, hoy en día, ofrecer una solución tecnológica al concepto jurídico de firma electrónica avanzada. Una simple aclaración en torno a los términos firma electrónica y firma digital. La primera es una expresión más genérica; y, la Firma Digital es aquella firma electrónica que está basada en los sistemas de criptografía de clave pública (PKI) que satisface los requerimientos de definición de firma electrónica avanzada.

Desde mi punto de vista e interpretación jurídica, los términos en referencia vienen a ser sinónimos, y por tanto identificaré como Firma Electrónica, con sustento normativo de nuestra Ley de Comercio Electrónico, FIRMAS ELECTRÓNICAS y Mensajes de Datos ***(las mayúsculas son mías)***.

Los programas de comunicaciones relacionados con la firma electrónica: son las denominadas aplicaciones de firma electrónica, las más importantes:

---

[84] *Definición según el art. 2 de la directiva 99/93 de la Comisión Europea, en el I Congreso Mundial de Informática y Derecho.*

[85] ***ALAMILLO, Ignacio;*** *La Firma Electrónica y los Requisitos.*

*** S/MIME,** para correo electrónico que firma y comprueba firmas, permitiendo comunicaciones de forma segura. Se emplea en pedidos comerciales por correo.

*** SSL (Secure Socket Layer),** aplicación para el protocolo HTTP para hacer seguras las conexiones web. Es decir, se emplea como elemento de seguridad para el comercio electrónico. Lo profundizaré más adelante.

*** SSH.-** aplicación para emplear un terminal de ordenador a distancia, de forma segura.

*** SET.-** aplicación desarrollada por VISA y MASTERCARD para el pago por medios electrónicos[86].

La firma electrónica, y sus aplicaciones, nos ofrece dos elementos de valor añadido:

1. Integridad del mensaje, es decir, poder determinar si el mensaje ha sido o no alterado.
2. Autenticación de la persona firmante, es decir, que conocemos el origen del mensaje (esto es válido aún cuando no tenemos a la persona identificada, pues la garantía de identidad la ofrece el propio certificado, no la firma).

La firma electrónica como está planteada se basa en dos principios del comercio electrónico: **La equivalencia funcional,** es decir, los mensajes de datos cumplen la misma función jurídica que una declaración de voluntad oral, escrita o gestual y **la neutralidad tecnológica,** es decir, la posición que adopta el Estado al momento de adquirir insumos y servicios tecnológicos y si debe existir o no preferencia hacia una u otra tecnología.

Por lo tanto, desde el punto de vista jurídico, es necesario asegurar: que el mensaje proviene de la persona que dice lo envía; que no ha sido alterado en el camino; que el emisor no podrá negar su envío ni el destinatario su

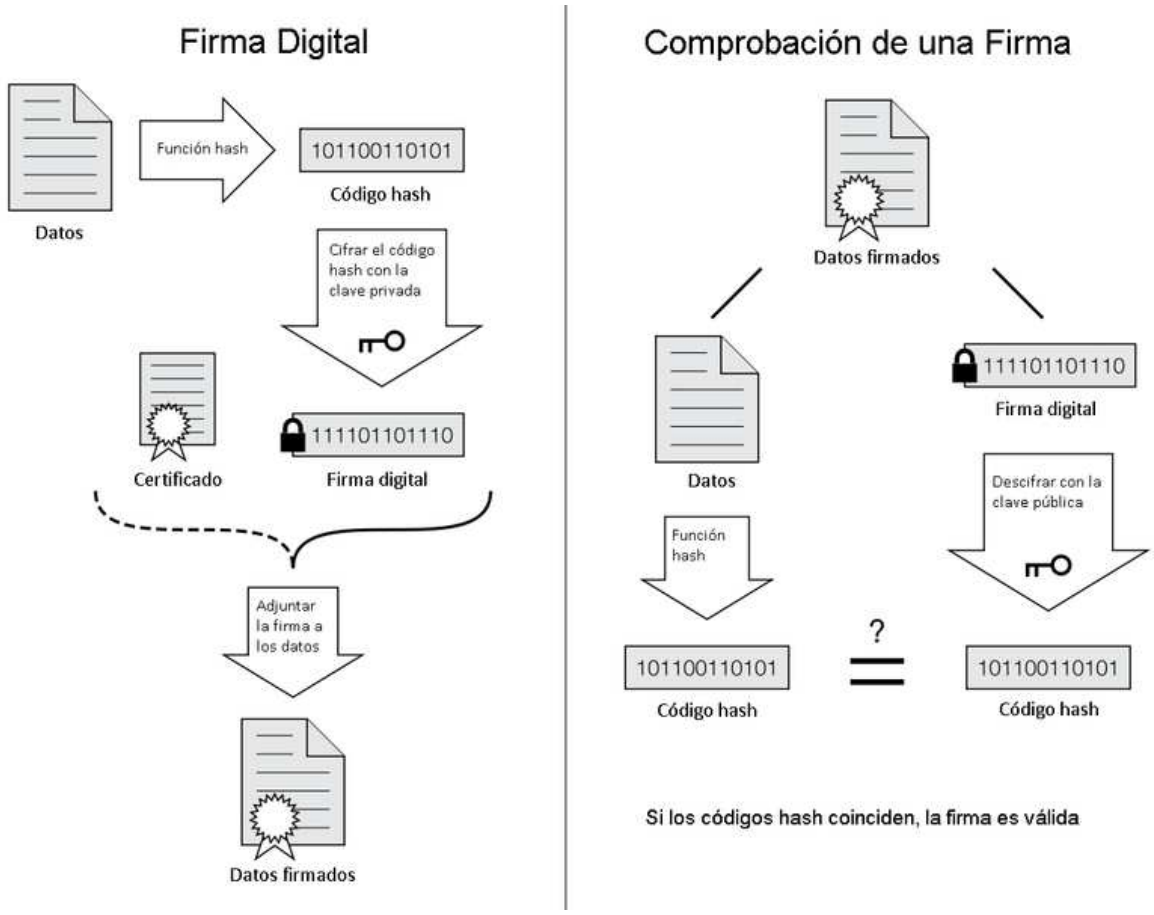
[86] ***Aplicaciones de Firma Electrónica,*** *aporte tomado del trabajo: Confianza Digital Basada en Certificados; por* ***ALAMILLO, Ignacio.***

recepción; y, en su caso, garantizar su confidencialidad. La satisfacción de estas exigencias jurídicas se consigue con la Firma Electrónica, que aporta los siguientes servicios de seguridad: ***la autenticación:*** asegura la identidad del remitente del mensaje; ***integridad,*** garantiza que el mensaje no ha sido alterado en el tránsito; ***no repudio*** en origen y en destino, garantiza que una parte interviniente en una transacción no pueda negar su actuación; y ***la confidencialidad,*** que protege los datos de revelaciones o accesos de terceros no autorizados.

Finalmente, y desde un punto de vista jurídico y conforme lo establece la Ley 67, la Firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio[87].

Véase el cuadro a continuación es la representación de cómo funciona la Firma Electrónica.

[87] ***Art. 14.- Efectos de la Firma Electrónica;*** *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; Actualizada a Agosto de 2007, Corporación de Estudios y Publicaciones.*



Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a. Ser individual y estar vinculada exclusivamente a su titular;
b. Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;
c. Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.
d. Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,
e. Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a. Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b. Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c. Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d. Verificar la exactitud de sus declaraciones;
e. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
f. Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g. Las demás señaladas en la Ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a. Voluntad de su titular;
b. Fallecimiento o incapacidad de su titular;
c. Disolución o liquidación de la persona jurídica, titular de la firma; y,
d. Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

4.3. P.G.P. (Pretty Good Privacy)

Es un programa desarrollado por Phil Zimmermann, cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales[88].

PGP, es una aplicación de alta seguridad criptográfica que puede ser utilizada bajo varias plataformas (MSDOS, UNIX, VAX/VMS), nos permite intercambiar archivos o mensajes con privacidad, autenticidad y conveniencia, es decir, que la privacidad y la autenticidad es dada sin la necesidad del manejo de llaves asociadas con programas convencionales de criptografía. Con PGP no se necesitan canales seguros para intercambiar las llaves entre los usuarios, lo cual hace más fácil su utilización; esto es porque PGP está basado en una tecnología llamada criptografía de llave pública[89].

Por lo tanto, función principal es “esconder información” a ojos de otras personas que quieran tener acceso a ella. Su uso más común es con el correo electrónico. Cuando se envía un mensaje de correo electrónico, ese mensaje pasa por muchos ordenadores antes de llegar a su destinatario y cualquier persona con acceso a esos ordenadores y con malas intenciones podría tener entrada a los mensajes. Usando PGP los mensajes no viajan tal como se escribieron, sino que van codificados, decodificándose únicamente en su

[88] ***http://es.wikipedia.org Pretty Good Privacy*** *o PGP (Privacidad Bastante Buena).*
[89] ***GAYNOR, Martin;*** *Pretty Good Privacy (PGP)*

destino. Por ejemplo, un texto que diga "Hola, soy yo" quedaría convertido en algo parecido a "DXCfg%/yfggER$%"[90].

PGP funciona con dos claves o 'keys':

1. Una pública que se autogenera y que es la que tienes que intercambiar con otros usuarios para poder mandar mensajes encriptados, y
2. Una privada que consiste en una frase de al menos 4 ó 5 líneas por ti elegida, y que la escribirás cada vez que quieras desencriptar algo.

Cuando alguien nos vaya a enviar un mensaje cifrado con PGP tendrá que encriptarlo con nuestra clave pública que le habremos proporcionado previamente.

Obviamente, para utilizar PGP es necesario tenerlo instalado en nuestro ordenador, un sitio de internet para descargar este programa es http://kriptopolis.com, el más sugerido y utilizado por expertos en la materia.

Siguiendo las instrucciones que aparecen en pantalla, el programa genera nuestras claves pública y privada durante el proceso de instalación. Al generarse estas claves, PGP nos pide un password para poder luego desencriptar información. Estas claves están ubicadas en la carpeta del programa, que por defecto es:

c: Program FilesPGPPGP55i

Clave pública: pubring.pkr

Clave privada: secring.skr

Al cerrar el programa PGP se nos invita a crear una copia de seguridad de las claves (lo más recomendable es hacerlo). Seguidamente exportaremos nuestra clave pública para poder entregarla adecuadamente a los que nos vayan a enviar mensajes codificados. Para ello hay que abrir el programa PGP Keys, ubicado en INICIO/PROGRAMS/PGP/PGP Keys. Se selecciona nuestra clave y

[90] ***Seguridadysitemas.com;*** *FAQ básica sobre el programa de encriptación PGP.*

se pulsa en KEYS/EXPORT, en ese momento aparece un cuadro de diálogo pidiéndonos donde guardar la clave. Ese archivo es el que deberemos enviar como nuestra clave pública.

Ahora bien, para poder enviar un e-mail o cualquier tipo de información encriptado. Lo primero que hay que hacer es obtener la clave pública de la persona a la que enviaremos el mensaje. Una vez con su archivo de clave pública en nuestro ordenador hay que importarlo a PGP Keys. Para ello:

- Colocaremos el archivo en una carpeta (por ejemplo la del PGP),

- Abrimos PGP Keys (INICIO/PROGRAMS/PGP/PGP Keys)

- Pulsamos KEYS/IMPORT

- En la ventana de diálogo se selecciona el tipo de archivo de la clave (.txt/asc/pkr/skr...) y se importa (este proceso se hace una sola vez).

Ahora si listo para enviar correo encriptado.

- Lo primero es abrir el programa de correo, ejemplo Netscape Messenger). Compondremos el mensaje normalmente, poniendo la dirección electrónica y el asunto en su sitio y el texto en el cuerpo del mensaje.

- Una vez el texto acabado se selecciona y con las teclas CONTROL+X se corta al portapapeles.

- Seguidamente pulsaremos en el icono que está junto al reloj de Windows en la barra de tareas (icono con un sobre blanco en el centro). Si no tenemos ese icono, lo podemos activar pulsando en INICIO/PROGRAMS/PGP/PGPtray.

- Del menú emergente se pulsa en "Encrypt Clipboard".

- En ese momento nos pregunta con qué clave queremos encriptar el texto. Seleccionamos la clave de la persona a la que vamos a enviar el mensaje haciendo doble click sobre ella. Seguidamente se pulsa en OK. En ese momento el contenido del portapapeles queda encriptado.

- Pulsamos de nuevo en el cuerpo del mensaje, que estará en blanco, y con las teclas CONTROL+V pegaremos el contenido del portapapeles al cuerpo del mensaje. Observaremos que el mensaje ahora es una serie de caracteres sin ningún sentido.

- Procederemos entonces a enviar el mensaje normalmente vía e-mail.

¿CÓMO DESENCRIPTAR UN MENSAJE QUE ME HAN ENVIADO?

Se procede abrir el mensaje y se ve que el mismo esta encriptado, procedemos a copiarlo íntegro al portapapeles:

-----BEGIN PGP MESSAGE-----

Version: PGPfreeware 5.5.3i for non-commercial use

<http://www.pgpi.com>

qANQR1DBwU4DhZrHKiEmOtwQCACKcH+Cw1r2zcCaN6PAH5sK1ZjX5J4C1GjU8Q9G

ajMEhvbHEB9tpbjfBD3UO5oZ8QFBvCaWIgZtg9cF317OfA5UaIhArInzPMRxgmPD

cHpciZS+83EMkZGcMjFAZfqMgCQgb0+Is1Ng6rCtRqdRAZlpmr7ABCIe1QeEG+6P

P79vzE3yf0JihVjSWz6dfAQ9nmyHDkRSA9p8VCdBKOXK9xPZMufjnHTSBRdxHCHz

EyRGmYIM1HrmFc+ZXQDBJy84X0VwnPazIlLjaJnpHd9OExvGIcer5LHE66Gu2WTP

UAnMw08QySNLgg6n2Uph+lKroCFvuG/W2toIWbGG+1TtbCxaA10IO7o7SQ==xtLd

-----END PGP MESSAGE-----

Incluyendo las líneas:

-----BEGIN PGP MESSAGE-----

..

-----END PGP MESSAGE-----

Seguidamente pulsamos en el icono PGPtray y seleccionamos la opción "Decrypt/Verify Clipboard". En ese momento se nos solicita el password para poder utilizar nuestra clave privada. Al introducirlo veremos en pantalla el texto original[91].

A manera de conclusión, puedo decir y según lo manifestado que este programa de seguridad, es el de más alto nivel de seguridad, su uso más frecuente es en el correo electrónico; encriptando textos o cualquier otro tipo de archivos, existe cantidad de comentarios sobre las vulnerabilidades que supuestamente tiene PGP, diciendo que no es seguro y que se puede romper, CLARO QUE SE PUEDE ROMPER, pero tras trillones de milenios de cálculos por cada mensaje.

Por lo tanto si alguien intercepta el mensaje PGP que me envían o envío a otra persona. Lo único que obtendrá es un conjunto de caracteres extraños sin pies ni cabeza que no podrá desencriptar, pues no posee la clave privada que es la pieza necesaria para poder convertir el mensaje a su forma original.

4.4. SSL Secure Socket Layer

Protocolo de Capa de Conexión Segura (**SSL**), es un protocolo criptográfico que proporcionan comunicaciones seguras por Internet.

El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar

[91] ***Seguridadysistemas.com;*** *FAQ básica sobre el programa de encriptación PGP*

futuras transacciones. MD5 se usa como algoritmo de hash.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP[92].

SSL es el estándar mundial de la seguridad en Internet. Además de evitar la manipulación de la información confidencial, esta tecnología ofrece a los usuarios la garantía de tener acceso a un sitio Web válido. SSL es compatible con los principales sistemas operativos, aplicaciones Web y hardware de servidor, lo que significa que esta tecnología de cifrado de SSL eficaz le ayuda a implementar en su empresa una capa de seguridad que limita la responsabilidad para todo el sistema con el fin de afianzar la seguridad de los clientes, aumentar el porcentaje de transacciones finalizadas y maximizar los beneficios.

SSL se convirtió en el estándar mundial hace más de una década para garantizar la privacidad de las comunicaciones en línea. El proceso consiste en crear un archivo de datos especial llamado certificado SSL para un servidor específico en un dominio y para una entidad concreta. Los certificados SSL son emitidos por entidades de confianza como VeriSign. Todas las entidades que reciben un certificado SSL se deben someter a algún tipo de autenticación que permita comprobar que son quienes dicen ser.

Con el aumento considerable del phishing y otras actividades fraudulentas en Internet con el objetivo de apropiarse de la información personal de otros usuarios, la autenticación de la identidad se convierte en un aspecto más importante que nunca. El nivel de autenticación de la identidad de un certificado SSL varía según el tipo de certificado SSL y la autoridad de certificación (CA).

Con SSL, un sistema de claves privadas o públicas cifra la conexión entre dos partes como, por ejemplo un usuario y un sitio Web con un certificado SSL. Si el explorador del cliente señala un sitio Web con SSL, un protocolo de enlace seguro entre ambos sistemas autentica ambas partes. En cada sesión se usa una clave de sesión única para el cifrado (cuanto más larga sea la clave, mayor será el nivel de cifrado). Una vez establecida la conexión, ambas partes

[92] ***www.iec.csic.es: Web Seguro,*** *Secure Socket Layer SSL.*

pueden iniciar una sesión segura a la vez que garantizan la privacidad e integridad de sus comunicaciones. Esta seguridad es especialmente importante si los usuarios comparten información confidencial en Internet, una extranet o incluso en una intranet. En el caso del comercio electrónico, una conexión SSL segura es fundamental para hacer negocios, ya que la mayoría de los usuarios de Internet temen compartir la información con un sitio Web que no ofrezca protección SSL[93].

El protocolo SSL permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente. La idea consiste en interponer una fase de codificación de los mensajes antes de enviarlos por la red. Una vez que se ha establecido la comunicación, cuando una aplicación quiere enviar información a otra computadora, la capa SSL la recoge y la codifica, para luego enviarla a su destino a través de la red. Análogamente, el modulo SSL del otro ordenador se encarga de decodificar los mensajes y se los pasa como texto plano a la aplicación destino.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

[93] ***VeriSing, Documento Técnico;*** *Los últimos avances de la tecnología SSL.*

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes fases:

1. La fase **Hola**, para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.
2. La fase de **autenticación**, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).
3. La fase de **creación de clave de sesión**, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.
4. Por último, la fase **Fin**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies

enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras HTTP.

Una comunicación SSL, por tanto, se resume así:

1. Fase de saludo (*handshaking*). Consiste básicamente en una identificación mutua de los interlocutores, para lo cual se emplean los certificados X.509[94]. Tras el intercambio de claves públicas, los dos sistemas escogen una clave de sesión, de tipo simétrico.

2. Fase de comunicación. Aquí se produce el auténtico intercambio de información, que se codifica mediante la clave de sesión acordada en la fase de saludo.

Cada sesión SSL lleva asociado un identificador único que evita la posibilidad de que un atacante *escuche* la red y repita exactamente lo mismo que ha oído, aún sin saber lo que significa, para engañar a uno de los interlocutores[95].

Gracias a los avances recientes de la tecnología SSL, existe una amplia variedad de tipos de SSL, pero el más importante para Internet es SSL Extended Validation (EV), estos tipos de certificados facilitan las operaciones en línea en todos sus aspectos, aumentando la confianza de los visitantes en los sitios y reduciendo en gran medida la eficacia de los ataques de phishing.

La arquitectura EV se ha diseñado para ofrecer una información de identidad fiable de un sitio Web a los consumidores finales de forma que puedan tomar las mejores decisiones con respecto a los sitios que desean visitar. El cumplimiento de esta misión requiere la modificación de todos los componentes de la arquitectura de confianza de la Web. Además de las nuevas convenciones de interfaz, los certificados EV deben su fiabilidad a:

1) **la modificación en los procedimientos de autenticación,** según directrices CA/Browser Forum, requiere que las autoridades de certificación utilicen información autenticada o primaria en lugar de información propia de los solicitantes del

[94] ***X509.-*** *Un certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, para demostrar que una clave pública pertenece a un usuario concreto.*

[95] ***LUCENA LÓPEZ, Manuel de Jesús,*** *Criptografía y Seguridad en Computadores, Segunda Edición Septiembre 2009, Departamento de Informática; Escuela Politécnica Superior Universidad de Jaén*

certificado. Utilizan técnicas de eficacia probada que cuentan con millones de certificados autenticados correctamente durante una década. Este procedimiento asegura que toda la información que contiene el certificado es exacta y que el solicitante del certificado tiene la autoridad para obtener este certificado para esta organización. Estos procedimientos de autenticación están disponibles para su examen público en www.cabforum.org. Todas las autoridades de certificación deben someterse a una auditoría anual por una empresa auditora adscrita a WebTrust, con el objeto de asegurar que cumple correctamente las directrices de EV; y,

2) **la comprobación de certificados en tiempo real,** Esta comprobación depende de dos infraestructuras paralelas. La primera es OCSP, mencionada anteriormente. OCSP realiza una comprobación de revocación en tiempo real de cada certificado, de forma que si un certificado EV está comprometido o si por cualquier otro motivo requiere una revocación, ese certificado no aparecerá como válido en navegadores compatibles con EV. El segundo servicio en tiempo real es Microsoft® Root Store. Un marcador de metadatos muy simple que indica el estado de cada certificado. Para protegerse de la posibilidad de que una autoridad de certificación sin principios o incompetente pueda emitir certificados incorrectos marcados como EV, incluso si no se han sometido a una autenticación EV correcta, el navegador IE7 realiza una comprobación en tiempo real de Microsoft Root Store para comprobar que esta raíz SSL está aprobada para certificados EV.

El propósito de los certificados SSL es validar la identidad de un sitio cuando un usuario se conecta. Los creadores concibieron el certificado como fedatario de la identidad de un sitio y protector de los clientes del fraude en línea. Un sitio Web puede incluso utilizar un certificado SSL emitido por sí mismo y no por una

autoridad de certificación, de ahí entonces que la autoridad certificadora reconocida es VeriSign[96].

4.5. Los Bienes Jurídicos Protegidos en el Delito Informático

El medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorción, robo, fraude, suplantación de identidad, y demás conductas delictivas conforme se ha visto en este trabajo. La investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta.

Según las estadísticas del mes de Septiembre del 2008 de la Superintendencia de Telecomunicaciones, en Ecuador hay alrededor de 1´329.713 usuarios de Internet, quienes corren un alto riesgo de ser perjudicados mediante actos delictivos como la ingeniería social, estafa, un ataque de phishing u otros, relacionados con las tecnologías. Las cifras sobre estos delitos en Ecuador son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos.

Es necesario antes que nada determinar el concepto de bien jurídico, para una mejor y amplia comprensión de esta temática en cuestión.

El ***Bien Jurídico*** es la elevación a la categoría de "bien tutelado o protegido por el derecho", mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido".

Para un sector de la doctrina el "delito informático" no es más que la comisión de actos delictivos mediante el uso de medios informáticos, es decir, se trataría de lesionar bienes jurídicos ya protegidos en la legislación penal, únicamente el medio es el que cambia.

---

[96] ***Confianza web mediante SSL,*** *Documento Técnico VeriSign, como aumentar la confianza de los visitantes web mediante SSL con EV.*

Otro sector de la doctrina opina que estos delitos tienen un contenido propio, afectando así un nuevo bien jurídico, LA INFORMACIÓN, diferenciando así los delitos computacionales (hardware y software) y los delitos informáticos propiamente dichos.

De lo dicho anteriormente, en nuestra legislación si existe sanción para este bien jurídico tanto en la ley 67 art. 58 en concordancia con el art. 202.1 Delitos contra la información protegida, y art. 202.2 Obtención y utilización no autorizada de información, del Código Penal , no obstante, en nuestra Constitución art. Art. 16 numeral 2 dice: acceso universal a las tecnologías de la información y comunicación. Por razón natural entonces, se puede interpretar que todos los ecuatorianos tenemos derechos a inmiscuirnos “en esta nueva era digital o revolución tecnológica”, siempre y cuando no atentemos contra los bienes jurídicos protegidos de las personas y el Estado mismo.

Determinado el bien jurídico protegido, se puede interpretar que, en el caso de los delitos informáticos, los múltiples posibles ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales. ¿Entonces qué es lo que nos separa de una correcta aplicación de las leyes penales preestablecidas? Sólo la pretendida falta de legislación en materia de delitos informáticos, y digo pretendida porque esto no es así, ya que al perpetrarse el delito a través del uso de medios informáticos no se está sino en presencia de un nuevo método comisivo del delito y no como erróneamente se piensa de un nuevo delito que para que lo sea debe estar correctamente tipificado. De ahí entonces, que para la aplicación de la norma existente, respecto de la comisión de un delito ya tipificado como tal, bastaría una “correcta” interpretación judicial por parte del juzgador, puesto que lo único que ha “cambiado del delito”, es el medio, utilización o forma tecnológica

En resumen, los delitos informáticos, en su gran mayoría dependen, para su persecución penal de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, por ejemplo, que si mañana se pudiese quitar la vida a alguien por medio de internet habría que establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica.

Muñoz Conde indica que la norma penal tiene una función protectora de bienes jurídicos y que para cumplir dicha función, eleva a la categoría de delito, por medio de la tipificación legal, aquellos comportamientos que más gravemente los lesionan o ponen en peligro

Así de esta forma, se entiende que el bien jurídico en los delitos informáticos directos es la información digital o electrónica, es decir, la que ha sido almacenada o la que está contenida en medios informáticos y/o electrónicos. ***Hugo Carrión***[97] indica que la información tiene interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.)[98].

Sin embargo, de lo dicho, no solo la información es el bien jurídico vulnerado, sino que tras este o paralelamente hay la concurrencia de una serie de bienes jurídicos "alterados", que en síntesis y solo por mencionar hay: derecho a la intimidad, a la privacidad, confidencialidad, honor e imagen, reputación, etc.,

---

[97] ***Tesis presentada por el Dr. Hugo Daniel Carrión*** *(Abogado Especialista en Derecho Penal).*

[98] ***FUENTES BELTRÁN, Patricio Fernando Dr. y FUENTES BELTRÁN, Soraya Viviana Dra.;*** *Derecho Informático, www.derechoecuador.com, generada el 15 de Febrero del 2010*

etc.; mismo que están tipificados en nuestra legislación con la única "desventaja o problema", no se expresa en la norma los medios utilizados.

Se puede decir entonces que dentro de los delitos informáticos, la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente[99].

El profesor Francisco Bueno Aruz en un estudio sobre el delito informático, respecto de los bienes jurídicos que pueden resultar afectados con los delitos informáticos, afirma:

"..., la cuestión de sí la delincuencia informática supone la aparición, en el mundo de la dogmática penal, de un nuevo bien jurídico protegido merecedor de protección específica, se convierte en algo relativo. Pues, si la novedad de esta delincuencia radica fundamentalmente en los medios utilizados (que ciertamente pueden hacer más dificultosa la averiguación y la prueba de los hechos), el bien jurídico protegido en cada caso será el que corresponda a la naturaleza de la infracción cometida: la intimidad, la propiedad, la propiedad intelectual o industrial, la fe pública, el buen funcionamiento de la Administración, la seguridad exterior o interior del Estado[100].

Toda tipificación de delitos, pretende proteger bienes jurídicos, así por ejemplo, respecto del hurto, el bien jurídico protegido es la propiedad. En el caso del homicidio, el bien jurídico protegido es la vida.

---

[99] ***ACURIO DEL PINO, Santiago;*** *Profesor de Derecho Informático de la PUCE; Delitos Informáticos: Generalidades.*

[100] ***CASTRO OSPINA, Sandra Jeannette,*** *Delitos Informáticos: La Información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano.*

En el caso de estos delitos informáticos, el bien jurídico que ha "surgido" por el uso de las modernas tecnologías es: la calidad, pureza e idoneidad de la información contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Sin embargo, y como ha se dijo anteriormente, no solo se protege ese bien sino que además concurren otros, tales como el **patrimonio,** en el caso de los fraudes informáticos; **privacidad, intimidad y confidencialidad de los datos,** en el caso del espionaje informático; **la seguridad y fiabilidad del tráfico jurídico y probatorio,** en el caso de la falsificación de datos probatorios vía medios informáticos; **el derecho de la propiedad sobre la información y sobre los elementos físicos materiales de un sistema informático,** en el caso de los delitos de daños, entre una extensa gama más; y reiterando e insistiendo en algo puntual y preciso, lo único que ha cambio es el medio de cometimiento del delito hoy llamado Informático, por lo que una vez más la Interpretación debe basarse en torno a los delitos "tradicionales".

Entonces a manera de conclusión se puede decir que "el interés social digno de tutela penal sería: ***La Información*** **-**almacenada, tratada y transmitida a través de sistemas informáticos**-** sin perjuicio que de ella deriven o traiga consigo una gama extensa de bienes jurídicos tutelados y protegidos por el derecho y legislación de cada país.

CONCLUSIONES

Una vez finalizado este trabajo y luego de todo lo analizado y estudiado en el mismo, se ha podido llegar a las siguientes conclusiones:

1. En un primer momento la informática fue utilizada de manera noble puesta al servicio de la comunidad con fines leales y lícitos, pero a medida que pasó el tiempo y se fue generalizando, comenzaron a surgir ciertas conductas o comportamientos delictivos vinculados a ella; es decir, se transformó en objeto de acciones ilícitas y pasó a ser utilizada como medio para la concreción de delitos.
2. El espacio virtual genera una atmósfera de anonimato que protege, promueve y alimenta nuevos modos de atentar contra las personas e instituciones. Además, por la propia constitución de la red, las conductas delictivas adquieren una potencialidad lesiva que viene a multiplicar los posibles daños a terceros.
3. Con el creciente avance tecnológico, las nuevas plataformas de comunicación digital han experimentado con especial intensidad los efectos tanto positivos como negativos generados por la globalización. El espacio virtual de Internet constituye, sin duda, una aldea global en la que el entramado de redes y la proliferación de nodos repercuten de forma inmediata en las relaciones humanas. En este contexto, nos hallamos ante el reto de enfrentarnos a nuevos canales especialmente proclives para la comisión de delitos, a novedosas formas comisivas que, como se ha visto, poseen una mayor capacidad lesiva. Más aún, se puede afirmar que se ha iniciado una nueva etapa, distinta, en la lucha contra la delincuencia, caracterizada por lo que se viene denominando la globalización del delito.
4. Las nuevas realidades de la tecnología y la informática que se han venido desarrollando en este mundo globalizado debido a su acelerado y vertiginoso avance, así como su incidencia directa en varios ámbitos de la sociedad han alcanzado el rango de bienes jurídicos protegidos por el ordenamiento jurídico, particularmente por el Derecho Penal. Por lo que

una vez más nos hace pensar que estamos en presencia de un proceso de transnacionalización del Derecho Penal, donde gracias a la globalización se ha logrado realizar esfuerzos para la creación de un sistema garantista capaz de proteger los derechos de la información.

5. Para que este sistema garantista del Derecho Penal de la Tecnología y la Información surta sus efectos, es necesario el compromiso de la comunidad internacional a fin de que regulen sus ordenamientos jurídicos de una manera uniforme siguiendo las recomendaciones y pautas señaladas por las diferentes organizaciones mundiales, y de esta manera se logre la armonización de sus legislaciones, para que los usuarios de la tecnología de la información se vean cada vez más protegidos y accedan al maravilloso mundo del ciberespacio.
6. La posibilidad de incompetencia de los jueces, la imposibilidad de extradición, la garantía del juez natural reconocida por los tratados internacionales de derechos humanos y otras anexas, como el debido proceso y el in dubio pro reo, presentan límites infranqueables para una legislación que no haya sido debidamente planificada en función de todas y cada una de ellas para otorgar una protección efectiva a los perjudicados y cumplir la función preventiva de que se nutre el derecho penal. Es claro que si los posibles infractores comprenden las imposibilidades de aplicación de las normas penales será muy fácil para ellos evadirlas y resultar así en la directa inaplicabilidad del sistema.
7. Sin duda alguna, el avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos utilizando medios tecnológicos generará una nueva generación de profesionales que darán respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos, y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información.
8. Es indudable que los países latinoamericanos están tomando iniciativas que les permite desarrollar estrategias para el seguimiento de los delitos informáticos, por ejemplo Argentina y Colombia han elaborado y aprobado las respectivas regulaciones que protegen el bien jurídico: la

información; entonces, Ecuador que cuenta ya con el entidad de Certificación de las Firmas Electrónicas, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos; así como iniciativas que permiten el seguimiento de ciertos aspectos tecnológicos, debe embarcarse en un proyecto que permita delinear aspectos regulatorios sobre las tecnologías de la información.

9. Una vez resuelto el problema de la Ley aplicable, corresponde al ordenamiento interno de cada país, según las normas de derecho penal internacional o interno la determinación del Juez Competente en cada caso en particular, pero con la salvedad de que en caso de no estar determinada por el ordenamiento interno, debe siempre estarse a los jueces de competencia nacional.

10. En el rubro de temas pendientes encontramos que en la legislación Ecuatoriana no se ha tipificado un delito contra la interceptación de telecomunicaciones y el abuso de dispositivos, de igual manera no se ha tipificado la posesión de material pornográfico infantil. A raíz de todo lo expuesto surge la imperiosa necesidad de legislar y así regular el grave problema de los delitos informáticos cada vez más comunes en estos días. Es sumamente trascendente el dictado de legislaciones que rijan los diferentes aspectos de las nuevas tecnologías,

11. Uno de los principales problemas que enfrenta la propiedad intelectual, es la piratería y falsificación de las obras del intelecto humano, las cuales traen graves consecuencias económicas y sociales; sumado a los perjuicios de los titulares de derechos de propiedad intelectual, pues esta pérdida afecta a los fabricantes de los productos falsificados, y a la reducción de ingresos tributarios e inclusive la pérdida de empleos, debido a los efectos negativos resultantes de la mano de obra clandestina, de las labores creativas y de investigación, perjudicando la vitalidad cultural y económica de un país.

Es deber del Estado y en especial de la Fiscalía el de promover las dinámicas sociales, jurídicas, tecnológicas, policiales, o de cualquier otra índole para hacer frente de forma eficaz al problema de la delincuencia informática. Así

como deber y obligación de jueces y magistrados actualizarse en torna a esta normativa para su correcta interpretación y aplicación de la ley.

De igual forma el Estado debe velar porque las aplicaciones de la tecnología sean correctas en el marco de la legalidad y de la ética, partiendo de bases y principios comunes que sean aceptados por la comunidad global, única manera de tener y mantener una verdadera protección al derecho a la intimidad.

RECOMENDACIONES

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación.

Luego de analizar la realidad de los delitos informáticos en el Ecuador y exponer mecanismos y herramientas existentes para su investigación, recomiendo considerar por sectores, algunos aspectos que desde mi punto de vista deben adoptarse en nuestro país: Gubernamental, Marco Legal, formación, tecnología y sociedad; los siguientes:

GUBERNAMENTAL

1. Establecer y alinear una política de lucha en contra de la delincuencia informática.
2. Incentivas mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar el delito informático que traspasa las fronteras de las naciones.

MARCO LEGAL

1. Proyecto de Ley de Delitos Informáticos.
2. Revisión de la Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital.
3. Reformas al Código de Procedimiento Penal del Ecuador sobre penalizaciones a las infracciones informáticas.
4. Establecer mecanismos de protección penal respecto de la delincuencia informática.
5. Desarrollo de proyectos que permitan llevar a cabo las recomendaciones del Grupo de Expertos Gubernamentales – Delitos Cibernéticos de la OEA.

FORMACION

1. Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Abogados) sobre los delitos informáticos y la informática legal.
2. Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc.
3. Fomentar el desarrollo de programas que involucren la disertación del peritaje informático, legislación existente que atañen a la informática, criminalística.
4. Desarrollo de programas de especialización que contemplen profesionales en informática forense y/o legal que pueden darse en cooperación con organismos especializados o entre convenios universitarios.

TECNOLOGÍA

1. Convenios institucionales (universidades, gremios, etc.)
2. Cooperación y transferencia de conocimiento con países vecinos, o con quienes se hayan establecido convenios internacionales, sobre la tecnología existente o el desarrollo de las mismas que permitan la persecución de los delitos informáticos.
3. Implementación de laboratorios especializados forenses informáticos.

SOCIEDAD

1. Advertir a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos.
2. Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico.
3. Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos.

4. Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.

El proceso de construcción de una Sociedad de la Información altamente eficiente y segura; "libre de una Ciberdelincuencia", será posible o por lo menos se podrá luchar contra estos expertos informáticos; si tomamos conciencia de la magnitud de sus alcances y consecuencias, así como en forma conjunta con todos los actores sociales trabajar y proponer acciones, tales como:

1. Levantar, procesar, actualizar e integrar una base de datos en la que se lleven registros de casos de delitos informáticos.
2. Difundir y sensibilizar a la sociedad sobre la aplicación del Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos.
3. Difundir la norma de calidad de los servicios de Internet que ha sido aprobada por el CONATEL.
4. Desarrollar e implementar una campaña de difusión con los proveedores de Servicio de Internet, telecentros y cibercafés, para crear conciencia en sus usuarios sobre los riesgos y cuidados que deben de tener en el manejo informático e Internet.
5. Desarrollar políticas de seguridad informática, para prevenir y denunciar esta clase de delitos informáticos.

Por otro lado, y como aspecto muy importante, sin decir con esto que todo lo anterior manifestado carece de trascendencia vital, Incorporación al ordenamiento jurídico nacional, de cuerpos legales internacionales sobre Ciberdelincuencia, especialmente la Convención Europea de Cybercrimen, la Convención de las Naciones Unidas contra la delincuencia transnacional y la Estrategia Interamericana Integral de Seguridad Cibernética. Mismo que por su amplio contexto y relevancia internacional servirá de pilar fundamental para que nuestros juzgadores apliquen e interpreten de mejor manera nuestras leyes. Así como la creación en la Fiscalía de la Unidad de Delitos Informáticos que establezca mecanismos de coordinación y cooperación con similares de otros países.

BIBLIOGRAFÍA

- **ACURIO DEL PINO, Santiago Dr.;** del Ministerio Público de Pichincha; Delitos Cibernéticos y Cibercriminalidad.
- **ACURIO DEL PINO, Santiago,** Delitos Informáticos y Cibercriminalidad.
- **ACURIO del Pino, Santiago,** Perfil Sobre los Delitos Informáticos en el Ecuador; documento guía para la VI Reunión del Grupo de Trabajo en Delito Cibernético de la REMJA, que se realizó el 21 y 22 de Enero del 2010 en Washington D.C.
- **ACURIO DEL PINO, Santiago;** Profesor de Derecho Informático de la PUCE; Delitos Informáticos: Generalidades.
- **ALAMILLO, Ignacio, Aplicaciones de Firma Electrónica,** trabajo: Confianza Digital Basada en Certificados.
- **ALAMILLO, Ignacio;** La Firma Electrónica y los Requisitos.
- **ARREGOITIA LOPEZ, Siura Laura;** Protección contra los Delitos Informáticos en cuba; Facultad de Derecho. Universidad de La Habana
- **CABANELLAS de Torres,** Diccionario Jurídico Elemental: Actualizado, corregido y aumentado; 17ª. Ed. – Buenos Aires: Heliasta 2005.
- **CASTRO OSPINA, Sandra Jeannette,** Delitos Informáticos: La Información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano.
- **CÓDIGO CIVIL,** Legislación Conexa, Concordancias, actualizada a octubre 2008.
- **CÓDIGO DE PROCEDIMIENTO PENAL,** Legislación conexa, Concordancias, actualizada a mayo de 2009.
- **CÓDIGO PENAL,** Legislación Conexa, Concordancias, actualizada a agosto 2008.
- **CÓDIGO ORGÁNICO DE LA FUNCIÓN JUDICIAL.**
- **CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR,** Comentarios, Legislación conexa, Concordancias, actualizada a mayo de 2009.

- **CORREL SEAN, Paúl; CORRONS, Luis;** El Negocio de los Falsos Antivirus: Análisis del Nuevo Estilo de Fraude Online; PandaLabs Julio 2009**.**
- **DELGADO López, Miguel,** Análisis Forense Digital, Página 5, 2da Edición, 2007
- **DOMÍNGUEZ GRAGERA, María Luisa.-** Normativa Aplicable a la Firma Electrónica (Directiva 99/93) Comercio Electrónico y Real Decreto- Ley 14/1999. Editorial La Ley. España. 2002. pp. 1339.
- **LANDAVERDE CONTRERAS, Melvin Leonardo,** Delitos Informáticos Universidad de El Salvador.
- **LEVENE, Ricardo;** Delitos y Tecnologías de la Información: Introducción a los Delitos Informáticos, Tipos y Legislación; Noviembre 2008- Argentina.
- **LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS;** Reglamentos, Legislación conexa, Concordancias, actualizada a agosto de 2007.
- **LINDOW, Diego Leonardo;** alumno de la Universidad Católica de Santiago del Estero; Delito Informático: Legislación, Represión y Prevención.
- **LUCENA LÓPEZ, Manuel de Jesús,** Criptografía y Seguridad en Computadores, Segunda Edición Septiembre 2009, Departamento de Informática; Escuela Politécnica Superior Universidad de Jaén.
- **MENESES DIAS, Cristian Andrés,** Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno, 30 septiembre 2002.
- **PEÑA Pérez, Pascal A.,** Delitos Electrónicos: Necesidad de una Ley que sancione los Crímenes y Delitos de Alta Tecnología en República Dominicana; Seminario “Delitos Informáticos en la R. D.” INTEC – 29 de Marzo, 2005
- **PROTECCIÓN CONTRA LA DELINCUENCIA INFORMÁTICA EN EL MERCOSUR,** por Marcelo Alfredo Riquert; Universidad Nacional de Mar del Plata.

- **REGIMEN DE PROPIEDAD INTELECTUAL,** concordancias; actualizada a 04 de enero del 2010.
- **SALOM, Genaro y ARTEGA, Valentín,** Delitos Electrónicos-Complicación.
- **SILVA SANCHEZ, Jesús María;** del trabajo realizado por Juan José González López, Artículos Doctrinales: Derecho Informático.
- **TINAJEROS ARCE, Erika Patricia,** Criminalidad Informática en Bolivia; Revista Informática Jurídica, Bolivia 2009.
- **URETA Arreaga, Laura Alexandra;** Retos a Superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador; Tesis de Grado Previa a la obtención del Título de: Magister en Sistema de Información Gerencial.
- **VALLEJO, María Cristina,** Fraude Informático; Revista Judicial, Abogada y Especialista Superior en Derecho Financiero y Bursátil, Ecuador/diciembre 2009.
- **YOSHI, Toranaga;** Fundamentos teóricos-doctrinarios de los Delitos Electrónicos, 25 enero 2008.

PAGINAS WEB

- **cert.inteco.es** Software Malicioso: Una Amenaza de Seguridad para la Economía de Internet.
- **eltiempo.com;** febrero 2009.
- **europa.eu:** Europa, Actividades de la Unión Europea síntesis de la Legislación: Lucha contra la Delincuencia Organizada-Lucha contra los Delitos Informáticos.
- **FUENTES BELTRÁN, Patricio Fernando Dr. y FUENTES BELTRÁN, Soraya Viviana Dra.;** Derecho Informático, www.derechoecuador.com, generada el 15 de Febrero del 2010.
- **Gómez Treviño Joel,** Delitos Informáticos; www.joelgomez.com.
- **http://es.wikipedia.org Pretty Good Privacy** o PGP (Privacidad Bastante Buena)**.**
- **http://es.wikipedia.org,** Wikipedia Le Enciclopedia Libre: Delitos Informáticos.
- **lalasoylala.blogspot.com:** Abuso Informático
- **mailxmail.com: Delitos Informáticos, capítulo 9:** Tipificación de los Delitos Informáticos.
- **Microsoft Encarta 2009.**
- **noticias.jurídicas.com:** Delitos Informáticos.
- **Seguridadysitemas.com;** FAQ básica sobre el programa de encriptación PGP.
- **Viruslist.com: Todo sobre Seguridad en Internet**, La carrera Armamentista en la Ciberdelincuencia.
- **www.alfa-redi.org**
- **www.alfa-redi.org** Revista de Derecho Informático: Los Delitos Informáticos; por Julio Núñez Ponce.
- **www.alfa-redi.org:** Revista de Derecho Informático, Acceso no autorizado a Sistemas Informáticos.
- **www.asobancaria.com** Phishing
- **www.conatel.gov.ec;** La Certificación de Información de la firma electrónica cuenta con regulación del CONATEL.

- **www.eumed.net** Seguridad en Internet.
- **www.ice.gov**
- **www.iec.csic.es: Web Seguro,** Secure Socket Layer SSL.
- **www.mailxmail.com**
- **www.rompecadenas.com** Ciberdelincuentes a la Cárcel.
- **www.tuabogadodefensor.com Comunicado de Prensa:** Lucha contra la Delincuencia en Internet, Abril 2008.
- **www.tuabogadodefensor.com Delitos Informáticos y Tecnológicos:** Los Delitos Informáticos en el Código Penal Español.
- **www.univision.com** con el título **Ligar en internet puede salir caro,** las redes sociales son usadas para timar.
- **www.usbank.com** Fraude por Correo Electrónico: Información y Ayuda.
- **www.wikipedia.com** La Enciclopedia Libre