UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA
UNAN-LEÓN

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Monografía para optar al título de Licenciatura en Derecho

TEMA

Los Delitos Informáticos y la Información como nuevo bien jurídico protegido

AUTORES

Bismarck Rodríguez Madrigal
Fabio Ernesto Flores Vázquez
María Lissett Berríos Reyes

TUTOR

Lic. Luis Hernández León.

León, Junio del 2006.

Agradecimientos:

Agradecemos en primer lugar por lograr haber concluido esta monografía a Dios nuestro creador quien con su amor y bondad nos ha acompañado en cada momento de nuestras vidas.

Agradecemos a nuestros queridos padres por habernos apoyado incondicionalmente y por habernos procurado siempre lo que en realidad ha sido lo mejor para nosotros.

Agradecemos a cada uno de los maestros de la facultad quienes a nuestro paso por las aulas de la Facultad nos han inculcados los conocimientos del Derecho que hoy nos hace ser los nuevos profesionales del Derecho de Nicaragua.

Agradecemos especialmente a nuestro tutor, el profesor Luis Hernández por su abnegable disposición, por su apoyo, por todo el tiempo que nos dedicó, por su gran generosidad y sobre todo por ser el gran maestro que es.

Nuestro agradecimiento no podría de ninguna forma ser menor con todo el personal de la biblioteca “Mariano Fiallos Gil” de nuestra facultad, por toda la voluntad y carisma de servicio demostrado en todo este tiempo. Por toda la paciencia con la que se revistieron para prestarnos libros y computadoras un millar de veces. A todos ellos; los Licenciados Luvy, Horacio, Martha, Aracelly, Marianito, a todos nuestros agradecimientos.

DEDICATORIA:

Dedico esta monografía a mis padres Luis Rodríguez y Eleuteria Madrigal.

A quienes les debo mi existencia, mi educación y mis sueños.

Bismarck Antonio Rodríguez.

Dedicatoria:

Dedico esta monografía a mi Madre Yolanda Isabel Reyes Aguilar, porque gracias a su esfuerzo y dedicación ha sido posible que mi educación llegue hasta este punto, el de poder optar ahora al título de licenciatura en Derecho.

Para ella mi amor y mi gratitud.

María Lissett Berríos Reyes.

Dedicatoria:

Dedico esta monografía primeramente a :

DIOS: por haberme dado la sabiduría, fortalezas e iluminarme el sendero para mi formación integral.

A mi madre Esther Vásquez Martínez de la cual he recibido todo el apoyo incondicional para que sea una persona de bien y que sirva a la sociedad.

A mi hermana Iveth Carolina flores Vásquez, la cual me motiva seguir superando en esta vida.

Para ellos mi agradecimiento, por ser la fuente de mi inspiración y alcanzar un peldaño mas en mi vida.

Fabio Ernesto Flores Vásquez.

INDICE

INTRODUCCIÓN.

Tal y como se nos dijo en nuestros primeros días de estudio en las aulas de esta facultad, el Derecho es la forma de las formas sociales, por que el derecho es una ciencia social y por eso va al ritmo del desarrollo de la sociedad y la sociedad se desarrolla al ritmo que avanza el conocimiento humano, o sea al ritmo de la ciencia. Por las razones expuestas es que debemos percatarnos de las novedosas situaciones que nos hace experimentar el progreso tecnológico que el siglo XXI ha traído consigo. La telemática[1] es parte de la vida diaria de las persona de países desarrollados o no. En los países de Norteamérica, Europa y algunos de Asia, un altísimo porcentaje de personas tienen computadoras en casa conectadas a Internet y en países poco desarrollados como Nicaragua, cada vez más aparecen cyber-cafés con costos cada vez mas accesibles y por ello son cada vez más las personas que empiezan a conectarse a Internet, bien sea para usarlo como medio de comunicación o como fuente ilimitada de información. Las empresas en su mayoría, basan su funcionamiento a redes de computadoras, en las que se registra la información importante para las futuras operaciones, los bancos en Nicaragua y en la mayoría del resto del mundo realizan sus transacciones a través de redes internas nacionales e internacionales, razón por la cual aparecen los cajeros automáticos y las tarjetas de crédito y de débito. Todo sin dejar de mencionar el impacto que sobre todo esto ha tenido la aparición de la fibra óptica.

Es claro que toda esta situación descrita trae muchas ventajas, ha simplificado, y agilizado muchas operaciones. Por ejemplo mucha gente ya no necesita ir a hacer enormes filas al banco, porque puede ir directamente al cajero automático y en cuestión de segundos hacer el retiro de dinero. Por otro lado un destinatario nuestro que vive en Francia, no necesita una semana para recibir nuestra correspondencia, ya que el correo electrónico llegará en fracciones de segundos.

[1]Ciencia que reúne y combina las posibilidades técnicas y los servicios de la telecomunicación y la informática.

El aspecto negativo que nos corresponde mencionar ahora, es una constante en la actitud del ser humano a través de toda su historia. Todas estas ventajas que han traído el desarrollo de la tecnología informática y del Internet aparte de beneficiarnos, nos ha puesto en una situación vulnerable ante la existencia de personas que sin escrúpulo alguno y con los conocimientos necesarios, con el objeto o no de sacar un provecho económico pueden mediante el uso de computadoras o tecnología semejante y haciendo uso de la red (Internet) realizar acciones perjudiciales que en esta monografía llamaremos delitos informáticos.

Primeramente, en el primer capítulo abordamos de manera general el Derecho informático, como nueva rama del Derecho, producto del desarrollo de la tecnología en este siglo y del impacto que eso ha tenido en la sociedad. Principalmente también por ser de esta nueva rama de donde surgen los delitos informáticos.

Luego abordamos directamente los delitos informáticos. Sus generalidades como conceptualización, clasificación, características, etc. Pero donde nos detenemos cuidadosamente, es ante la pregunta de que si en delitos informáticos existen o no nuevo bien jurídico protegido, por lo que presentamos en este capítulo algunas posiciones doctrinales opuestas.

También nos referimos de manera mas detallada a algunas de los delitos informáticos mas conocidos y mas frecuentes. Hacemos énfasis particular en la pornografía infantil y en el terrorismo en Internet por ser hechos que reiteradamente se promueven en la red, lo cual nos resulta condenable desde todo punto de vista.

Finalmente, para dar una idea clara del desarrollo que el tema ha tenido en otros países, presentamos la legislación que en algunos de los países de Europa y el continente americano se ha desarrollado sobre Delitos informáticos, concluyendo

con un análisis del marco legal nicaragüense que atañe a los Delitos informáticos, y sobre todo el proyecto del código penal, que contiene algunas innovaciones en cuanto al tema, encontradas en ciertos artículos dispersos en todo el código.

CAPITULO I
GENERALIDADES

1. La naturaleza social del Derecho.

Todas las ciencias que integran el conocimiento humano, suelen clasificarse de acuerdo al tipo de fenómeno que estudian. Así ciencias que tienen por objetos de estudio a fenómenos naturales se denominan ciencias naturales y tendrán las características de sus objetos de estudio. De igual forma las ciencias que se desempeñan en el estudio de fenómenos sociales[2]. Dentro de las primeras están la física, la química, la biología, etc. Dentro de las segundas junto a la filosofía, sociología, la economía, se encuentra el Derecho.

Una vez establecida la naturaleza social del Derecho con relación a su objeto de estudio, queda establecer la naturaleza misma de este objeto de estudio. Los fenómenos sociales están determinados por la forma de actuación de los seres humanos[3]. Es decir comprenden aquellas transformaciones que de u modo u otro afectan la estructura o funcionamiento de la sociedad. Por lo tanto el Derecho, ya sea entendido como ciencia o como el fenómeno jurídico producido por el desarrollo de la sociedad humana[4], va a ser dinámico cambiante, no estático ni exacto, dada la naturaleza fluctuante de la sociedad.

Tomando en cuenta lo anterior, podemos entender la tendencia del Derecho a adaptarse a los cambios sociales significativos que demandan reestructuración o modernización del Derecho positivo. Ejemplo de ello, sería la aparición del Derecho mercantil en un momento en el que surge una clase social cuyo actuar

[2] Introducción al estudio del Derecho / Monjarrez S. Luis; Ed. Universitaria, 2003. Pág. 17
[3] Ídem
[4] Ídem

económico no encuadraba de manera satisfactoria en el viejo Derecho civil[5]. El auge del comercio en esa época, el gran desarrollo del cambio y del crédito fueron entre otras las causas que originaron la multiplicación de las relaciones mercantiles, que el Derecho común era incapaz de regular en las condiciones exigidas por las nuevas situaciones y necesidades del comercio[6].

Otro buen ejemplo que podríamos ilustrar, es el derecho laboral, su surgimiento y las condiciones en que lo hace. Tiene sus primeras manifestaciones a finales del siglo xix, con la creación inorgánica de legislaciones sociales en Europa y América. A comienzos del siglo xx, el desarrollo del movimiento sindical, el auge que experimentaron los derechos sociales, la creación de la OIT, y la generalización de formas democráticas de gobierno (voto universal), crearon las condiciones para una nueva institucionalidad de las relaciones laborales que produjo la aparición de un "nuevo derecho", el Derecho laboral, como rama separada del Derecho civil y con principios jurídicos propios y novedosos. El Derecho laboral aparece así ligado a la recién nacida idea de "justicia social", con un carácter fuertemente protector de los derechos de los trabajadores, habitualmente la parte débil de la relación laboral. El Derecho laboral se configurará como el corazón del naciente "Estado de bienestar[7]. Vemos pues que las variaciones en la sociedad, traen consigo también variaciones en el Derecho buscando este siempre marchar en armonía con el ritmo de marcha de la sociedad.

Es claro que un fenómeno no es social, sin la intervención del ser humano. Por ende no cabe la menor duda de que el boom tecnológico que experimentamos hoy en día, se reviste de un carácter social. Es sorprendente el acelerado ritmo que ha venido teniendo el desarrollo de la tecnología a partir del siglo XX, pero dentro de la misma tecnología, la parte de ella que se encarga del almacenamiento, tratamiento y transmisión de la información (La tecnología informática), es la que

[5] Curso básico de Derecho mercantil / Navaz M. Azucena / Ed. Universitaria, 2004. Pág. 20
[6] http://www.monografias.com/trabajos14/derecho-mercant/derecho-mercant.shtml
[7] http://es.wikipedia.org/wiki/Derecho_laboral

ha puesto aprueba una vez más el carácter dinámico del Derecho naciendo de esta forma el Derecho informático.

2. El Derecho informático.

2.1 Concepto.

El concepto de "Derecho Informático" (Rechtinformatik) fue acuñado por primera vez por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania en la década de los Setenta.

El Derecho informático está integrado por las disposiciones legales que regulan el tratamiento automático de la información, en los países sen donde tales normas existen. Dicho esto, no podemos hablar de tal concepto aplicándolo al Derecho positivo nicaragüense, sin embargo esto no resta validez científica a la doctrina internacional que sobre el tema se ha venido desarrollando.

En concordancia con lo anterior, citamos a Enrique Pérez Luño[8], quien define el Derecho informático como una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos, integrado por el conjunto de disposiciones dirigidas a la regulación de nuevas tecnologías de la información y comunicación (informática y telemática.

Un concepto más conciso nos lo ofrece el Dr. Héctor Peñaranda Quintero[9], juez venezolano y presidente de la organización mundial de Derecho e Informática, y que define el Derecho informático como "Una ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio

[8] http://comunidad.derecho.org/gmontoya/
[9] http://www.monografías.com/trabajo23

informático en su expansión y desarrollo, y b) Aplicación idónea de los instrumentos informáticos".

Finalmente presentamos la definición que se hace en la enciclopedia "Wikipedia"[10], la cual nos ha perecido muy práctica y objetiva": El Derecho informático es un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la Informática. Rama del derecho especializado en la temática de la informática, sus usos y aplicaciones y sus implicaciones legales".

A diferencia de la "Informática jurídica", en la que la tecnología es vista meramente como herramienta o instrumento de apoyo para los diversos operadores jurídicos (abogados, estudios jurídicos, tribunales de justicia, cámaras parlamentarias, etc.), el "Derecho informático" se interesa en los fenómenos, hechos y consecuencias que surgen por el uso de las TICs en los procesos sociales, siendo como fuente de problemas jurídicos relevantes, así mismo el Derecho Informático busca proponer vías de solución y regulación adecuadas.

Así en los países en donde estas definiciones son válidas, existe un corpus[11] completo y coherente de normas legales que en sí misma, tienen la capacidad de dar solución de manera adecuada a los problemas jurídicos que el avance de la informática ocasiona.

El Derecho como eje fundamental sobre el que se estructura la sociedad, debe ocuparse claramente sobre este nuevo asunto que trae repercusiones sociales, hablamos de las relaciones cada vez más intensas, entre la tecnología y la información, tanto así que progresivamente van afectando desde las más simples hasta las más complejas actividades de nuestras sociedades.

[10] http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico
[11] Término latino de donde deriva la palabra cuerpo.

No por lo novedoso que es este nuevo objeto de regulación vamos a creer que la regulación no es la misma de la que se ejerce en ámbitos tales como las relaciones patrimoniales (Derecho civil) o la prevención y sanción de conductas que afectan los bienes jurídicamente tutelados (Derecho penal). Por eso es que Gustavo Montoya en su artículo publicado en Internet[12] afirma que: "El Derecho no sufre ninguna transformación fundamental por el embate de las nuevas tecnologías y por el contrario, ve asegurada su asepsia y su pureza".

2.2 *Informática jurídica y Derecho informático.*

La Informática Jurídica es básicamente una técnica en el tratamiento de información, por lo tanto al igual que ésta es de carácter jurídico bien podría ser de otra índole; de allí que en esencia sólo constituye informática aplicada al derecho, del mismo modo que se aplica a la medicina, la economía, la contabilidad o cualquiera otra materia. No es extraño, por ende, que los ingenieros informáticos lleguen a negar la existencia de la Informática Jurídica como disciplina independiente, ya que para ellos sólo existe la informática, sin calificaciones, aplicada en diversos campos.

Ahora bien, si la tecnología es lo central de este fenómeno, la verdadera transformación del Derecho no puede radicar únicamente en el uso subsidiario de instrumentos tecnológicos desarrollados por otras disciplinas, sino en que el derecho en si mismo y desde su propia esencia instrumentalice de manera práctica el conocimiento científico de base, con miras a realizar eficientemente sus fines y propósitos.

Así pues, el Derecho como tecnología, supone que éste se halle fundado necesariamente en conocimientos científicos así como que esté orientado a obtener eficientemente resultados prácticos, puesto que la tecnología no es sino la aplicación práctica del conocimiento científico.

[12]http://comunidad.derecho.org/gmontoya

Finalmente entender el Derecho como tecnología supone un cambio de perspectiva que hará posible que el Derecho desde su propia esencia pueda aprovechar convenientemente las ventajas de las nuevas tecnologías y ponerse a la altura de los tiempos garantizando y haciendo posible las imprescindibles condiciones de orden, control, seguridad, eficiencia y justicia que la sociedad requiere para una adecuada estructuración de las interacciones económicas, sociales y políticas[13].

3. Naturaleza del Derecho informático.

He aquí un asunto sobre el cual los más prominentes jurisconsultos latinoamericanos no se han puesto de acuerdo. En muestra de ello, les presentamos primeramente la postura del Dr. Gustavo Montoya M, catedrático de Informática jurídica en la Universidad central de Medellín, Colombia.

3.1 Naturaleza mixta del Derecho informático.

Según el Prof. Montoya el Derecho informático tiene naturaleza mixta, ya que es un Derecho público cuando se refiere a tres campos específicos, a saber: La regulación internacional de datos informatizados (aspecto internacional público), libertad informática y defensa de otras libertades individuales frente a eventuales agresiones provenientes de la tecnología informática (aspecto constitucional) y la delincuencia informática (derecho penal. Es derecho privado cuando se refiere a la contratación informática (Contratos cuyos objetos sean elementos de Hardware o Software), protección de software y comercio electrónico[14].

[13] http://comunidad.derecho.org/gmontoya/files/info04.htm
[14] Ídem

3.2 El Derecho informático como rama autónoma del Derecho.

Esta es la posición asumida por el Dr. Héctor Ramón Peñaranda Quintero[15], quien considera que el Derecho Informático no es una rama típica, pero sin embargo constituye conocimientos y estudios específicos que se encuentran entre la relación Derecho e Informática, pues para hablar propiamente de la autonomía de una rama del derecho se necesitan ciertas características: la existencia de campo normativo, docente, institucional y científico, con la finalidad de que se dé un tratamiento específico de estos conocimientos determinados, lo cual con un poco de estudio es posible observarlo en el Derecho informático[16].

No cabe duda entonces de que a pesar de lo incipiente de esta nueva rama jurídica, cumple con los requisitos señalados para que podamos nominarla de tal modo, por lo tanto no hay excusa ni siquiera en los países donde el grado de la tecnología de la información sea bajo, para que se obvie la posibilidad de hablar de Derecho informático como rama jurídica autónoma del Derecho.

4. Contenido del Derecho informático.

En realidad el Derecho informático no trata de nuevos problemas jurídicos, sino que se tratan en su mayoría de los mismos problemas tradicionales, vistos esta vez a través del lente de la tecnología y su más último desarrollo en el tratamiento de la información.

[15] Abogado, magíster en gerencia tributaria-Doctor en Derecho-Presidente de la organización mundial en Derecho informática. Autor del libro "Iuscibernética. Interrelación entre el Derecho y la informática". Es también juez del tribunal de protección del niño y del adolescente de la circunscripción judicial del Estado Zulia

[16] http://wwww.monograafìas.com/trabajos23/jurìdica-informàtica.shtml

4.1. Según el Dr. Marcelo Bauza.

En una forma muy lógica y sistemática, el Dr. Marcelo Bauza[17] ordena el contenido del Derecho automático de la siguiente forma:

4.1.1 –Derechos humanos:

a) Las libertades y derechos más preciados.
b) Derechos de la personalidad.
c) Derechos laborales.

4.1.2 –Derechos patrimoniales. Están referidos al campo de los bienes intangibles (soportes lógicos de la información, bancos de datos, sitios Web, nombres de dominio[18], firmas digitales, etc.)

4.1.3 – Derechos relativos a la circulación de bienes propiamente informáticos.

a) Contratos sobre bienes y servicios informáticos.
b) Responsabilidad civil informática.
c) Responsabilidad penal informática.

4.1.4 – Derechos relativos a la circulación de los bienes informáticos por medio de instrumentos informáticos.

[17] Krupskaya Nadiezda/Derecho informático: Contenido y aplicación. Facultad de ciencias jurídicas y sociales; UNAN-Leòn, 2003.

[18] Un **dominio** es la parte de una URL (dirección de una página o recurso en Internet) que identifica al servidor en el que se aloja (por ejemplo: wikipedia.org). Estos dominios se clasifican por temas según su terminación (o dominio raíz), de tal forma que los terminados en .com se destinarían a uso comercial, .org a organizaciones sin ánimo de lucro, gob a páginas gubernamentales, .edu a instituciones educativas, etc. También existe un dominio raíz para cada país del mundo, como .es para España, .mx para México, .arg. para Argentina, etc.

a) El acto y el negocio jurídico.

b) El derecho de la prueba operando en ambientes de firma digital y documento electrónico.

4.1.5 – Derecho público de la informática.

a) Cuestiones jurídicas sobre telecomunicaciones (telemática).
b) Contratación de bienes y servicios informáticos por parte del Estado.
c) Actividad administrativa automatizada.

4.2. *Según el Dr. Miguel Davara Rodríguez:*

El Dr. Davara Rodríguez hace una enumeración diferente del contenido del Derecho informático, partiendo no del tipo de derechos que se ven afectados sino enumerando los temas novedosos que le son propios a la materia.

4.2.1 – La protección de datos.

El Dr. Davara entiende la protección de datos personales como la protección que el Estado debe a sus ciudadanos contra la posible autorización no autorizada que terceros puedan hacer de dichos datos personales y que son susceptibles de usos no autorizados.

4.2.2 – Protección jurídica del software.

La protección jurídica del software no encuadra adecuadamente en la figura de la propiedad intelectual, mas bien compagina de mejor forma con los Derechos de autor, pues el convenio de Berna utilizó la frase “Cualquiera que sea el modo o forma de expresión”.

4.2.3 – Protección jurídica de la base da Datos.

Esta protección si se da a través de la figura de la propiedad intelectual, pues se trata de las relaciones contractuales entre creador y distribuidor, o entre distribuidor y usuario, regidas ambas relaciones por el principio de la Autonomía de la voluntad.

4.2.4 – La contratación electrónica:

La contratación electrónica es aquella que se realiza mediante la utilización de algún elemento electrónico cuando este tiene o puede tener una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo.

4.2.5 – Los contratos informáticos.

Esta es la parte del Derecho informático que regula la contratación de bienes o servicios informáticos, o sea realizados por medio de ordenadores, elementos informáticos, o incluso a través de la telemática.

4.2.6 – Transferencia electrónica de fondos.

El Derecho informático trata de regular aquí aspectos tan novedosos que por sí mismos podrían justificar la existencia del Derecho informático. Estamos hablando en este caso de las transacciones bancarias a través de Internet, el pago electrónico; el llamado dinero plástico, etc.

2.7 – Informática en el procedimiento.

La informática puede también jugar un papel fundamental en la ejecución misma del Derecho. Por tal razón se han hecho estudios para determinar el grado de

eficacia dela informática en la agilización de los procesos judiciales y por ende en la solución de problemas de la retardación de justicia.

4.2.8 – Documento electrónico.

Este es un tema sobre el que mucho se ha debatido hoy en día. El problema no es la determinación del concepto de documento electrónico, sino mas bien la determinación del grado de eficacia que tal documento tiene para el Derecho.

4.2.9 – La sociedad de la información y la normativa sobre telecomunicaciones.

Hay países que por su desarrollo ya tienen un alto número de personas naturales y jurídicas envueltas en un mundo en que la información se convierte en el eje principal de funcionamiento, por lo tanto el Derecho informático viene a tomar parte en el asunto.

4.2.10 – Los delitos informáticos.

He aquí en este último inciso el objeto principal de nuestra monografía. Es para nosotros ahora más fácil entender que el Derecho informático como auténtica rama autónoma del Derecho que además de tratar de dar soluciones normativas a las distintas cuestiones que eminentemente informáticas contengan repercusiones jurídicas, también prevea el quebrantamiento de sus normas, el ataque a los bienes jurídicos, algunos creados por él y otros solamente tutelados, por la tanto de esta forma claramente podemos ver como este novedoso término “Delitos informáticos” es parte del contenido de esta nueva rama autónoma del Derecho (El Derecho informático), del cuál en el presente capítulo dimos un ligero esbozo, para dar una idea clara del panorama en el que se encuentra ubicado el tema de nuestra investigación.

5. Tendencias internacionales de la informática y el Derecho.

Después de la evolución que ha tenido en los últimos años la materia, podemos establecer claramente tendencias, que se tienen en los distintos países del mundo[19], respecto del desarrollo de la informática y el derecho; de esta manera podemos enumerar las siguientes tendencias, las cuales cuentan cada una de ellas-, con sus características particulares, así tenemos: inicial o básica, progresiva o creciente, avanzada o próspera y culminante o innovadora.

A) Tendencia Inicial o Básica: 1) Poco avance y desarrollo de la informática jurídica y del derecho informático, debido a la escasa importancia dada a la materia por los profesores de derecho de las Universidades y también por los funcionarios del Gobierno. 2) Se empieza a promover que se incluya la materia de informática jurídica en los planes de estudio de las facultades de derecho, desarrollo inicial de la doctrina nacional (se estudia al Derecho informático, dentro de la informática jurídica).

B) Tendencia Creciente o Progresiva: 1) Distinción clara entre informática jurídica y derecho informático, como ramas totalmente independientes una de la otra, pero relacionadas entre sí; se empieza a desarrollar en firme, la doctrina nacional al respecto. 2) Consideración del Derecho informático como rama autónoma del Derecho; incluyéndose en los planes de estudio de las principales facultades de derecho del país, de manera separada a la materia de informática jurídica; en Europa se recomienda aglutinar a ambas materias bajo la concepción "informática y derecho", en virtud de considerar más completa esta definición.

C) Tendencia Avanzada o Próspera: 1) Destaca la necesidad e importancia de desarrollar la labor legislativa respecto al Derecho informático, normas específicas que regulen su aplicación; auge importante respecto a la doctrina y jurisprudencia al respecto (Ej. delitos informáticos no tipificados en los códigos penales, etc.).

[19] http://www.alfa-redi.org/rdi-articulo.shtml?x=398

2) Desarrollo y consolidación importante de la legislación, doctrina y jurisprudencia nacional del derecho informático; controversia de casos prácticos nacionales e internacionales en la Corte Suprema del país.

D) Tendencia Culminante o Innovadora: 1) Avances importantes en respecto de la informática jurídica metadocumental, auge de centros de investigación para la utilización de sistemas de inteligencia artificial aplicados al derecho, desarrollo de tesis doctorales relativas a la inteligencia artificial y el derecho. 2) Desarrollo de proyectos prácticos y específicos de utilización de la inteligencia artificial aplicados al Derecho.

6. Tendencias de la informática y el Derecho en el Derecho comparado.

Con el fin de determinar las tendencias que presentan algunos países en particular, respecto de la informática y el derecho -analizaremos en forma breve-, algunos países de Europa y América Latina, agrupándolos por el tipo de tendencia que en nuestra opinión refleja la situación en que se encuentran en la actualidad, aclarando que dicha clasificación se encuentra sujeta a errores, debido a que no contamos con toda la información que quisiéramos, pero, sin duda alguna, marca un parámetro para futuras investigaciones[20]. Se tomó en cuenta el avance interno que han tenido en las siguientes áreas:

- Inclusión de la materia de informática jurídica y derecho informático en los planes de estudio de las facultades de derecho;
- Distinción clara entre informática jurídica y el derecho informático (el derecho informático como rama autónoma del derecho);
- Desarrollo de la doctrina nacional de la informática y el derecho;
- Propuestas, iniciativas y desarrollo de legislación que regule aspectos sobre derecho informático;

[20] http://www.alfa-redi.org/rdi-articulo.shtml?x=398

- Jurisprudencia sobre casos resueltos por la Corte Suprema;
- Centros de investigación sobre informática jurídica; y
- Centros de inteligencia artificial aplicados al derecho.

6.1 - Países con Tendencia Inicial o Básica:

Dejamos para una investigación posterior, el determinar que países efectivamente se encuentran en esta tendencia, ya que podríamos caer fácilmente en aseveraciones inciertas, por lo que preferimos clasificar solamente aquellos países que de alguna manera, es visible su desarrollo en informática y derecho.

6.2 - Países con Tendencia Creciente o Progresiva:

Venezuela.- El desarrollo de este país en cuanto a la informática y el derecho en general, con la información disponible, es relativamente poco.

Colombia.- La Universidad Externado de Colombia, cuenta con un departamento de informática jurídica que trabaja en la recopilación, clasificación, análisis y sistematización de legislación y jurisprudencia de los altos tribunales judiciales; el departamento ofrece a la comunidad su colección de bases de datos jurídicos en CD-ROM, una de las más completas de este país.

Brasil.- Cuenta con el Centro de Procesamiento de Datos de la República de Brasil (PRODASEN).

Perú.- En este país se lleva la materia de informática jurídica en la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima.

Chile.- Este país cuenta con el Centro de Informática Jurídica de la Facultad de Derecho de la Universidad de Chile, el cual se encarga del procesamiento y recuperación de información de las principales leyes de ese país. Respecto a la legislación del derecho informático, Chile ha emitido una de las pocas leyes de América Latina, que regulan los llamados delitos informáticos (LEY-19223), la cual

cuenta únicamente con 4 artículos, emitida por Enrique Krauss Rusque, Vicepresidente de la República, Santiago de Chile, 28 de mayo de 1993.

Costa Rica.- En el aspecto legislativo sobre el derecho informático, tenemos que existe una propuesta de legislación del recurso del Habeas data, proyecto de ley que pretende reformar la Ley de la Jurisdicción Constitucional, con el fin de incorporar dicho recurso del Habeas Data en Costa Rica, el cual resulta interesante debido a que intenta recoger una necesidad sentida de proteger la intimidad, dignidad y autodeterminación de los ciudadanos frente a los retos que ofrece el procesamiento automatizado de datos personales.

6.3 - Países con Tendencia Avanzada o Próspera:

Argentina.- Cuenta con uno de los mejores bancos de datos legislativos de América Latina, el Sistema Argentino de Informática Jurídica, en el aspecto académico, se imparte en la Facultad de Derecho y Ciencias Políticas de la Universidad Católica de Buenos Aires, un "Postgrado de Derecho de la Alta Tecnología" -con duración de un año-, y también en la Facultad de Derecho y Ciencias Sociales de la Universidad de Buenos Aires, se ofrece un "Curso de Actualización en Informática Jurídica",

Por otro lado, en la Universidad del Salvador, se imparte la "Maestría en Ciencia de la Legislación", en forma conjunta con la Universitá degli Studi di Pisa, Dipartimento di Sienze della Politica de Italia, con una duración es de dos años de estudio. También existe en la Universidad Nacional de Lánus, la maestría denominada "Nuevas Tecnologías para la Justicia" -dividida en cuatro módulos-, la cual cuenta con profesores de Italia, Inglaterra, Francia, Argentina, Chile, Paraguay y Uruguay, así como funcionarios de justicia de Italia y Argentina.

En cuanto a la legislación sobre el derecho informático, es importante señalar que en este país, la Corte Suprema de Justicia, había ratificado los fallos de instancias inferiores que declaraban que no correspondía perseguir penalmente a quienes

reproducían programas sin el permiso del autor, en virtud de existir un vacío legal, el cual ha sido subsanado al emitirse la ley que pena la piratería del software. Los diputados de este país (comisiones de legislación penal, de comunicaciones, de ciencia y tecnología y de legislación general), en octubre del año pasado, se encontraban trabajando sobre un nuevo proyecto de ley sobre delitos informáticos, en dicho proyecto se toman en cuenta el acceso ilegítimo a datos, el daño y el fraude informático, entre otros temas.

Uruguay.- Cuenta con el CINADE (Centro de Informática Aplicada al Derecho), cuyo Director es el Dr. Marcelo Bauzá Reilly, en dicho centro se desarrollan importantes proyectos de la materia, tuvieron a su encargo el desarrollo del VI Congreso Iberoamericano de Informática y Derecho, celebrado en el mes de mayo del 1998. El Dr. Bauzá, recientemente, acaba de firmar convenios con la antes mencionada Red CHASQUI (adscrita al Programa Alfa de la Unión Europea), con la Universidad de Greenswich, Londres, y con la Universidad Nacional de Lánus, Argentina; lo anterior con el fin de promover estudios acerca de las nuevas tecnologías de la información para el jurista en su país.

6.4 - Países con Tendencia Culminante o Innovadora.

Están en la cúspide del desarrollo legislativo en cuanto a Derecho informático, el número de países que se incluyen en esta tendencia no es muy grande, así que vamos a referirnos a los más conocidos:

Estados Unidos.- En la actualidad cuenta con la mejor base de datos jurídica a nivel mundial (Lexis-Nexis), y existen proyectos desde hace años sobre el uso de la inteligencia artificial aplicada al derecho (p.e. el Taxman Ii de McCarty y Sheridan y el de la Rand Corporation de Waterman y Peterson), razón por la cual podemos establecer que se encuentra en la tendencia culminante o innovadora del desarrollo de la materia. Las demandas y juicios judiciales, debido a los temas propios derivados del derecho informático, son en realidad, incontables en este país.

España.- En este país, se vienen dando -desde hace varios años-, en las Facultades de Derecho de España, conferencias y simposios importantes sobre el uso que tiene la informática aplicada al campo del derecho; en este sentido, a través del Seminario de Informática y Derecho de la Universidad de Zaragoza, se han llevado a cabo y organizado, los 3 primeros Congresos Iberoamericanos de Informática y Derecho: El primero celebrado en Santo Domingo, República Dominicana (1984); el II (segundo), celebrado en Guatemala, Guatemala (1989); y el III (tercero), celebrado en Mérida, España (1992); por lo que coincidimos con el profesor Héctor Peñaranda, quien menciona que existen países desarrollados como España, en el cual sí se puede hablar de una verdadera autonomía en el Derecho informático y que aunque esta materia como rama jurídica apenas nace y se encuentra en desarrollo, se está perfilando actualmente como una nueva rama jurídica autónoma.

Es importante mencionar que en cuanto a la legislación que ha desarrollado España, sobre informática y derecho, destaca el proyecto de ley sobre firma electrónica que ha sido aprobado por la Unión Europea (compuesta por doce artículos y dos disposiciones), la cual se menciona que saldrá el próximo verano; para lo cual, se creara un carné de identidad para poder navegar con seguridad por Internet, y que surtirá la misma eficacia jurídica que una firma manuscrita sobre papel y será admisible como prueba para efectos procesales, a través de cualesquiera de los medios admitidos en Derecho, dicha firma electrónica tendrá el tamaño y el precio aproximado de una tarjeta de crédito y funcionará con un módem especial, de precio reducido.

Es pertinente mencionar que España cuenta con una "Maestría en Informática y Derecho", ofrecido por el Instituto Español de Informática y Derecho (IEID) y la Facultad de Derecho de la Universidad Complutense de Madrid, en la cual se estudian, por una parte, tanto a la informática jurídica como al derecho de la informática, y por otra, materias complementarias y prácticas en organizaciones y empresas. Por otra parte, el departamento de Derecho Político de la Facultad de

Derecho de la Universidad Nacional de Estudios a Distancia (UNED), ofrece un programa de estudios del Tercer Ciclo (Doctorado en Derecho), titulado anteriormente "Limitación Constitucional del uso de las Tecnologías Informáticas", el cual a cambiado recientemente de nombre, denominándose ahora "Derechos constitucionales e informática", dicho programa se encuentra adscrito al departamento de Derecho Político, el cual dirige Don Eugenio Ull Pont.

Francia.- Cuenta con el DEA de Informática Jurídica y Derecho de la Informática, de la Facultad de Derecho de la Universidad de Montpellier, actualmente se encuentra adscrita a la Red CHASQUI (perteneciente al Programa Alfa de la Unión Europea).

Italia.- País sumamente desarrollado en cuanto a la legislación sobre derecho informático; siendo el primer país que dio una solución integral al problema relativo a la autoridad de certificación, sobre la firma digital asimétrica, problema que ha desatado una gran competencia internacional en toda Europa, pues existen grupos y categorías que quisieran tener el monopolio de esta autoridad. Se llevan a cabo cada año, congresos internacionales sobre inteligencia artificial y Derecho.

Japón.- Este país se encuentra dentro de la quinta generación del desarrollo de la informática en el mundo, la cual considera la comunicación con la computadora en lenguaje natural y la utilización de sistemas expertos[21].

[21] Véase el trabajo del profesor Luke Nottage, de la Kyushu University Law Faculty (Fukuoka, Japón).

CAPITULO II

LOS DELITOS INFORMATICOS.

Toda investigación se desarrolla a partir de conocimientos sólidos y conceptos firmes. Es por ello que antes de hablar sobre delitos informáticos en la presente monografía, necesitamos diferenciarlos de los llamados delitos electrónicos, y para lograrlo vamos a necesitar diferenciar también la electrónica de la informática.

Diferencia entre electrónica e informática.

Según el diccionario Nuevo mundo de la lengua española[22], la electrónica es la ciencia que estudia los dispositivos cuyo funcionamiento está basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de los campos magnéticos.

Una definición similar encontramos en la enciclopedia on-line Wikipedia[23] : "La **electrónica** es una ciencia aplicada que estudia y emplea sistemas cuyo funcionamiento se basa en el control de flujo de electrones u otras partículas cargadas en una gran variedad de dispositivos, desde válvulas termoiónicas[24] hasta los semiconductores[25].

En cambio en las mismas fuentes bibliográficas citadas, la definición que encontramos de informática nos empieza a dar las pautas que necesitamos para encontrar diferencias entre ambos términos. "Informática es el conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la

[22] (Diccionario Nuevo Mundo Lengua Española – Ediciones Nuevo Mundo – Dirección Gustavo A. Dos Santos – España 1.999)
[23] http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico
[24] Termiónica consiste en la emisión de electrones por un conductor eléctrico calentado a temperatura elevada.
[25] Conductor eléctrico cuya resistencia disminuye al aumentar la temperatura.

información mediante máquinas computadoras (hardware) que funcionan con distintos programas (software)[26].

También se puede definir la informática como "La **Informática** es la ciencia del tratamiento automático de la información a través de un computador (llamado también ordenador o computadora)".

Informática es un vocablo inspirado en el francés *informatique*, formado a su vez por la conjunción de las palabras *information* y *automatique*, para dar idea de la automatización de la información que se logra con los sistemas computacionales.

Planteado los dos conceptos nos corresponde analizarlos para que hagamos nuestra propia conclusión. Está claro que todo aparato que funciona sobre la base de flujo de electrones es campo de estudio de la electrónica, o sea que podemos decir que televisores, celulares, equipos de sonidos e incluso computadoras, todos ellos aparatos que funcionan a base de la energía que produce le desplazamiento continuo de electrones, son objeto de estudio de la electrónica, con la salvedad que nos da el concepto de informática, en el que podemos apreciar que dentro de todos estos aparatos electrónicos hay un grupo de ellos que son materia específica de la informática por que a pesar de que funcionen a base del flujo de electrones, estos tienen una función especial y es el de tratar, transmitir, almacenar y procesar datos, hablamos de las computadoras y sus accesorios, por lo que en conclusión podemos afirmar que la electrónica es la ciencia general y la informática, la parte especial de ella dedicada a los aparatos electrónicos que procesan y almacenan información. En otras palabras todo aparato informático, es aparato electrónico, pero no todo aparato electrónico es un aparato informático.

[26] Diccionario Nuevo Mundo Lengua Española – Ediciones Nuevo Mundo – Dirección Gustavo A. Dos Santos – España 1.999

2. Diferencia entre delitos electrónicos y delitos informáticos.

Corresponde tras referenciar la significación idiomática analizar el marco conceptual en que ambos términos son utilizados. Para ellos vamos a seguir la cátedra que sobre el tema desarrolla el Profesor Argentino Gabriel Andrés Campoli[27]:

El marco conceptual a utilizar es: “por medio de” y “en contra de”

Muy difícil resulta alcanzar una exacta delimitación de la significación de los conceptos.

A tales efectos, distinguimos las siguientes construcciones gramaticales.

a) Delitos cometidos por medio de elementos electrónicos.

b) Delitos cometidos en contra de equipos electrónicos.

c) Delitos cometidos por medio de elementos informáticos.

d) Delitos cometidos en contra de equipos informáticos.

A continuación recurrimos a un procedimiento de descarte:

1°) Se advierte el hecho de que todos los equipos informáticos están construidos con elementos electrónicos y que no todos los equipos electrónicos son necesariamente equipos informáticos (recuerde Ud. su radio o su televisor) por lo que corresponde dejar de lado la opción d), toda vez que la misma se encuentra contenida dentro de la b) la cual, a su vez, es más amplia en su encuadre hermenéutico.

---

[27]  Profesor de Informática Jurídica y Delitos Informáticos en la Maestría en Procuración de Justicia – INACIPE – México.

2°) También se observa que sólo los equipos dotados de la capacidad de procesar datos pueden por regla general ser utilizados como medio comisivo de acciones que afecten bienes jurídicos que a la sociedad le pueda interesar brindarle mayor protección (la penal), ya que resulta muy difícil imaginar a un sujeto activo tratando de, por ejemplo, violar una cerradura electrónica de un banco por medio del uso de una radio o un teléfono celular (que son claros ejemplos de equipos electrónicos no informáticos), pero es fácil imaginar al mismo sujeto activo intentando similar acción por medio de un equipo portátil de procesamiento de datos u otro artefacto similar con la capacidad necesaria para generar en cortos lapsos de tiempo infinidad de claves numéricas.

Se impone de esta manera descartar la fórmula a) por resultar poco apropiada a los medios habituales de comisión de delitos y asimismo alejada de la realidad.

Nos quedan, así vigentes por omnicomprensivas las formulaciones b) y c), es decir Delitos cometidos en contra de equipos electrónicos y Delitos cometidos por medio de elementos informáticos.

Esto marca ya una notable diferencia entre las alocuciones utilizadas como delitos electrónicos y delitos informáticos.

2.1 - Los delitos comprendidos y el ámbito de aplicación de cada uno.

Para construir las bases de un sólido andamiaje jurídico es menester en este momento describir el ámbito de aplicación de cada uno de los casos bajo análisis.

Tenemos así que los delitos cometidos en contra de equipos electrónicos resultan pues aquellos en los cuales el receptor físico del daño impetrado por el autor resulta expresamente un equipo electrónico.

Muy torpe sería dentro de esta categoría pretender, por ejemplo, incluir el delito específico de daños reconocido en todas las legislaciones penales, por ejemplo en

aquellos casos en que alguien destruye un cajero automático, salvo que este tuviere que ver con destrucciones totales o parciales producidas a través de la utilización de medios informáticos.

En contraposición observamos los delitos cometidos por medio de elementos informáticos, los cuales presentan una variada gama que pasa por los daños, las injurias y calumnias, las estafas (las realizadas en subastas on line encabezan todos los listados conocidos) y otros muchos.

De esta diferencia notoria podemos extraer una quizás más sutil pero mucho mas científica, ¿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, etc.

Esta segunda diferencia arroja un poco más de luz en esta obscura telaraña de definiciones que nos viene envolviendo desde el inicio del presente.

Determinado el bien jurídico protegido, podremos inducir 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.

De este somero pero conciso análisis podemos inferir que las diferencias entre delitos electrónicos e informáticos se pueden plasmar de manera exitosa en los siguientes enunciados:

1. Que los delitos electrónicos e informáticos no resultan equivalentes y además los términos utilizados no son sinónimos.

2. Que todos los delitos electrónicos son perpetrados por medio del uso de la informática, razón por la cual no cabe menos que inferir que los delitos electrónicos son una especie del género de los informáticos.

3. En la mayoría de los casos, los delitos electrónicos constituyen una especie tan particular y específica que a la fecha, no se encuentran dentro del espectro penal vigente la protección del bien jurídico que se afecta, mientras que los delitos informáticos la poseen, ya que no son otra cosa que nuevos medios comisivos de delitos ya existentes.

Siguiendo esta línea de reflexión podemos precisar que el género delito informático reconoce, al menos, dos especies:

a) Delitos informáticos electrónicos
b) Delitos informáticos no electrónicos[28].

3. Definición de delitos informáticos.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo

[28] http://www.alfa-redi.org/rdi-articulo.shtml?x=1480

cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".

Aún así veamos algunas definiciones, como la que nos da Carlos Sarzana, en su obra Criminalista e tecnología. Él dice que los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos.

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador", siendo mayormente usados los dos primeros términos, pero como no son términos de igual significado los hemos diferenciado claramente para definirnos por usar únicamente el término Delito informático por ser el único verdadero objeto de nuestro estudio.

En este orden de ideas, en el presente trabajo se entenderán como "delitos informáticos" todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho penal, que hacen uso indebido de cualquier medio informático.

4. La información como bien jurídico.

Al hablar sobre diferencia entre delitos electrónicos y delitos informáticos quedó claro que en los primeros no se afectaba a más de un bien jurídico, el que resultaba ser la propiedad o mas bien la integridad física de los bienes inmuebles y por el contrario en los delitos informáticos se afectaba a más de un bien jurídico, hablábamos de varios, pero es en este apartado donde hablaremos de una aspecto pocas veces tratados anteriormente. ¿Existe un nuevo bien jurídico protegido en la tipificación de los delitos informáticos? ¿Es este nuevo bien jurídico la información?

4.1 Algunas posiciones doctrinales.

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 como tantas otras cuestiones jurídicas, en algo relativo. Pues, si la novedad de la mencionada 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.

"Ahora bien, si, por el contrario, se trata de delitos que recaen sobre objetos informáticos propiamente dichos (aparatos, programas, datos), en algunos casos, aunque no siempre, podremos considerar, con el profesor ROMEO CASABONA, la aparición de un bien jurídico nuevo: la información sobre la información, como algo que reviste por sí solo un valor (económico o ideal) lo suficientemente interesante como para que la conducta correspondiente sea merecedora de una calificación jurídica y de una sanción atendiendo exclusiva y preferentemente a la importancia de la información sobre la información..."

En el Primer Congreso Andino de Derecho e Informática, celebrado en marzo de 2001 en Venezuela, el Director de la Revista Electrónica de Derecho Penal, el profesor peruano Luis Miguel Reyna Alfaro, propuso en su ponencia que se incorporara como bien jurídico objeto de tutela la "información", en tratándose de conductas cometidas valiéndose de medios informáticos. Algunos de los argumentos expuestos en su escrito fueron los siguientes:

"..., el punto de partida y también de más difícil resolución es el de la identificación del bien jurídico penalmente tutelado, lo que nos lleva a escudriñar si el delito informático en realidad protege algún nuevo interés social, o a entender si el bien jurídico que pone en peligro el delito informático es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos)' ".

(...) "Los constantes avances tecnológicos en materia informática han propiciado los nuevos conceptos, generando así mismo la modificación de otros tantos, enriqueciéndolos la mayoría de ocasiones, así el contenido del término 'información', que según la información de la Real Academia Española significa: 'enterar, dar noticia de algo' y que en términos legos hubiera significado tan sólo una simple entrega de datos, se ha ampliado, transformándose como advierte Téllez Valdez: 'en un valor social valioso, con frecuencia dotado de autonomía y objeto del tráfico'.

"Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que 'la información' deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión)."

(...) "Así podemos decir que el objeto social digno de tutela penal sería: 'la información (almacenada, tratada y transmitida a través de sistemas informáticos),..."

4.2 La información como bien jurídico intermedio.

Esta es la posición que asume la Doctora colombiana en Derecho Sandra Jeannette Castro Opina[29], quien por la solidez de sus argumentos y la lógica de sus aseveraciones hemos decidido seguir en esta monografía, además de adherirnos a su posición:

La sanción por lesión de intereses colectivos necesarios para la comunidad, con el objeto de evitar la afectación de los derechos fundamentales de los individuos; es un criterio que se ha venido plasmando en el derecho penal a través de la regulación de los delitos de peligro.

Diversos sectores doctrinales han expuesto sus críticas con ocasión de la creciente legislación penal de peligro, cuando se trata de conductas que pueden afectar el medio ambiente, la seguridad del tráfico automotor, la salud pública, o el orden económico y social; entre otras. Argumentan que se trata de concepciones inmanentistas del bien jurídico; o que se omite este referente, interesando tan solo la observancia de la norma jurídica como objeto de protección, para evitar

[29] Profesora Titular de Derecho Penal de la Universidad Externado en Colombia.

disfuncionalidades en el sistema. Se ha planteado también, que con esta legislación no solo se desconocen los principios necesarios para la intervención del derecho penal, como los de lesividad y fragmentariedad; sino que se anticipa su intervención a etapas anteriores a la puesta en peligro de un bien jurídico perteneciente a un sujeto individual y concreto.

Pese a lo anterior, no puede desconocerse que las lesiones a los bienes jurídicos necesarios para la existencia digna del ser humano, no se circunscriben a las agresiones directas y personales; sino que pueden lograrse a través de ataques indirectos e impersonales. Para ilustrar esta reflexión, podría decirse que el bien jurídico de la vida puede afectarse tanto cuando se envenena a una persona con una sustancia tóxica que se vierte en un vaso con agua que beberá; como cuando se contamina el agua destinada para el consumo humano de una población. Ambos comportamientos deben evitarse y pueden ser sancionados por el derecho penal, pues teleológicamente tienen como referente al ser humano; pero la forma de regulación es diferente. En el primer caso, objetiva y subjetivamente, se sanciona la conducta que lesiona en forma directa el bien jurídico de la vida; en el segundo, es punible la contaminación del medio ambiente y en concreto el agua para consumo humano, como bien jurídico intermedio, que finalmente pretende proteger la vida de las personas.

Esta alusión a los bienes jurídicos intermedios, obliga a citar el estudio realizado por el Profesor Titular de Derecho Penal de la Universidad de Valladolid, Ricardo M. Mata y Martín, quien los definió así:

"Bienes jurídicos intermedios o de referente individual pueden considerarse aquellos intereses colectivos tutelados penalmente de forma conjunta con bienes de los particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque".

Sintetizando lo expuesto en el trabajo elaborado por el autor citado, podría decirse que son requisitos de los bienes jurídicos intermedios los siguientes:

- Son suprapersonales, es decir, superan los intereses particulares.
- Están vinculados a un bien jurídico netamente personal.
- Pertenecen a los "intereses de la comunidad" y no al ámbito de los "intereses del Estado", pues los primeros tienen una mayor relación con los bienes individuales.
- Son cualitativamente homogéneos con los intereses individuales que pueden resultar vulnerados; o se encuentran en una misma dirección de ataque del comportamiento punible. Por ejemplo, pureza del medio ambiente y vida o salud personal; o el atentado contra la seguridad del tráfico y la simultánea puesta en peligro de la vida o integridad de la persona.
- Hay una relación medial entre el bien colectivo y el bien individual; el primero es medio o paso previo necesario para la lesión o puesta en peligro del segundo. Hay entonces un bien jurídico-medio (colectivo) y un bien jurídico-fin (individual).
- La lesión de bien jurídico intermedio representa un riesgo potencial para un número plural e indeterminado de víctimas.
- La lesión al bien colectivo, como límite mínimo, no ha menoscabado de manera efectiva los bienes personales, que es el límite máximo. De esta manera se sobrepasa el estadio del peligro abstracto.

En nuestro criterio, el derecho a la información, es un bien jurídico intermedio, por reunir todos los requisitos aludidos:

En primer lugar, es un derecho colectivo o supraindividual, en su triple dimensión de confidencialidad, integridad y disponibilidad.

En cuanto a la confidencialidad debe decirse que, en la sociedad moderna, la comunidad tiene derecho a la privacidad de los datos atinentes a la vida personal de sus miembros; a las estrategias comerciales, publicitarias o mercantiles; a los secretos industriales; y las comunicaciones; entre otras. Este derecho se traduce en un sentimiento de seguridad y de tranquilidad en la convivencia social.

Así mismo, la colectividad tiene derecho a la autenticidad e integridad de la información. La falta de confianza en los medios y documentos electrónicos genera dificultades en el tráfico jurídico.

Por último, los miembros del grupo social tienen derecho a la disponibilidad de la información sin perturbaciones ni trabas, pues ella les permite ejercer libremente sus derechos. Solo el conocimiento hace posible la libertad.

Aplicando las características de los bienes jurídicos intermedios al ***bien jurídico información*** nos encontramos con lo siguiente:

- Tal y como ha sido definido, el derecho a la información es un interés de la comunidad y no del Estado.
- A través de los ataques al derecho a la información, en las dimensiones señaladas, se pueden afectar intereses individuales como la intimidad, el patrimonio económico, o la autonomía personal, que son cualitativamente homogéneos y se encuentran en una misma dirección de ataque del comportamiento punible.
- Hay una relación medial entre el derecho a la información como bien colectivo y los derechos individuales que pueden verse afectados. El primero es medio o paso previo necesario para la lesión o puesta en peligro de los segundos.
- La lesión del derecho a la información representa un riesgo potencial para un número plural e indeterminado de víctimas;
- La sanción por delitos que atenten contra el derecho a la información, en sus aspectos de confidencialidad, integridad y disponibilidad, no constituirían delitos de peligro abstracto; pues han lesionado el bien jurídico intermedio y, teleológicamente, se dirigen, en concreto, a afectar intereses individuales.

El considerar la información como bien jurídico intermedio, tal y como lo proponemos, permite de lege ferenda sancionar conductas que lesionan este derecho colectivo y ponen en peligro intereses individuales.

De lege lata, el estudio de los requisitos de los bienes jurídicos intermedios, permite hacer efectivo el principio de la antijuridicidad material en la subsunción de conductas y eliminar en la práctica la sanción de las catalogadas como de peligro abstracto. En los delitos cometidos por medios informáticos, antes de realizar la subsunción en el tipo que protege el bien jurídico individual, habría que analizar también si afectó el bien jurídico colectivo de la información en alguno de los aspectos mencionados (confidencialidad, integridad y disponibilidad)[30].

5. Características de los Delitos informáticos.

De acuerdo a las características que menciona en su libro Derecho Informático el profesor mexicano Dr. Julio Téllez Valdés[31], en donde se podrá observar el modo de operar de estos ilícitos, las características de los delitos informáticos son las siguientes:

- Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, en cuanto se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

[30] Artículo publicado en Internet en la siguiente dirección: http://www.delitosinformaticos.com/delitos/colombia1.shtml

[31] Doctor en informática jurídica y derecho de la informática por la Universidad de Montpellier. Francia.(http://highered.mcgraw-hill.com/sites/9701043065/information_center_view0/julio_tellez_valdes.htm)

- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- 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[32].

6. Elementos de los delitos informáticos.

Doctrinariamente hablando los delitos informáticos poseen los mismos elementos que los otros mas delitos, sino no serían llamados Delitos informáticos en los países en que están tipificados, pero por ahora básicamente los elementos más importante a nuestro interés son el sujeto activo (quien comete el delito informático) y el sujeto pasivo (el que de alguna manera ya sea directa o indirecta resulta perjudicado).

6.1 Sujeto activo en los delitos informáticos.

Las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los

[32] Artículo publicado en Internet en el siguiente sitio web: http://www.elrinconcito.com/articulos/DelitosInf/legisdelinf.htm

delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación labora se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos[33].

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, tendiendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la

[33] http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar[34].

[34] http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo35.htm

6.2 Sujeto pasivo de los delitos informáticos.

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el 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, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar 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, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que "para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, una análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más[35].

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

7. Clasificación de los Delitos informáticos.

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: Como instrumento o medio y como fin u objetivo[36].

7.1 Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.
b) Variación de los activos y pasivos en la situación contable de las empresas.

[35] http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm
[36] http://www.angelfire.com/freak2/dubi/DI.htm

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.
d) Lectura, sustracción o copiado de información confidencial.
e) Modificación de datos tanto en la entrada como en la salida.
f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h) Uso no autorizado de programas de cómputo.
i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l) Acceso a áreas informatizadas en forma no autorizada.
m) Intervención en las líneas de comunicación de datos o teleproceso.

7.2 Como fin u objetivo: en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Daño a los dispositivos de almacenamiento.
d) Atentado físico contra la máquina o sus accesorios.
e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc..

En lo que se refiere a delitos informáticos, Oliver Hance en su libro Leyes y Negocios en Internet, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

- Acceso no autorizado: es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.
- Actos dañinos o circulación de material dañino: una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).
- Interceptación no autorizada: en este caso, el hacker[37] detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

[37] Persona de grandes habilidades y conocimientos informáticos cuyo pasatiempo favorito es intentar acceder a sitios y sistemas informáticos sin autorización.

8. La clasificación que hace las Naciones unidas de los delitos informáticos.

En un estudio que las Naciones unidas hicieron sobre la prevención y control de los delitos informáticos, se muestra la siguiente clasificación de los delitos informáticos[38]:

8.1 Fraudes cometidos mediante manipulación de computadoras.

8.1.1 Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

8.1.2 La manipulación de programas: Es muy difícil de descubrir y a diferencia del anterior para cometerlos se requieren conocimientos mas sofisticados sobre informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

8.1.3 Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones

[38] Manual de las Naciones Unidas Nos 43 y 44, cuyas pautas se dieron en el congreso sobre prevención del delito, realizado en Viena del 15 al 17 de abril del 2000.

para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

8.1.4 Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es la famosa técnica especializada denominada técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Muchas veces puede efectuarse con abuso de confianza, pues es susceptible de realizarse por personal con acceso a los sistemas que manejan el flujo de capital a través de redes informáticas.

8.2 Falsificaciones informáticas.

8.2.1 Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

8.2.2 *Como instrumentos*: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

8.3 Daños o modificaciones de programas o datos computarizados.

8.3.1 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. Las técnicas que con mas frecuencia permiten cometer sabotajes informáticos son los virus informáticos, los gusanos informáticos y las bombas lógicas.

8.3.2 Accesos no autorizados: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

8.3.3 *Reproducción no autorizada de programas informáticos de protección legal*: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunos países han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, tenemos que decir que la le reproducción no autorizada de programas informáticos no es un delito meramente informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

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

a) Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
b) Infracción al copyright de bases de datos: uso no autorizado de información almacenada en una base de datos.
c) Interceptación de correo electrónico: Lectura de un mensaje electrónico ajeno.
d) Estafas electrónicas: a través de compras realizadas haciendo uso de la red.

e) Transferencias de fondos: engaños en la realización de actividades bancarias electrónicas.

Por otro lado, la Internet permite dar soporte a la comisión de otro tipo de delitos:

- Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes.

Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa[39].

9. Conductas informáticas ilegales más comunes.

Entre las conductas informáticas que se catalogan con más frecuencia de ilegal y prejuiciosas, están las siguientes:

[39] www.desolapate.com/Conferencia%20Delitos%20Informaticos.htm

9.1 Hacker: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos; 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Un hacker es un Apasionado de la tecnología, de todo tipo, quiere investigar cuanta cosa sale en el mercado. Experto en SO, sistemas de seguridad, programación avanzada, criptología, conocimiento de phreaking

El hacker puede actuar solo o en grupo, pero generalmente si se reúnen es para intercambiar información, no para que los demás miembros le enseñen a hackear.

La rutina para ellos es bajar todo lo que puedan de Internet sobre vulnerabilidad, sistemas operativos, ingeniería social, phreaking, programación. Inventan un nick (sobrenombre), para que los demás los reconozcan, y generalmente no transmiten desde su casa.

9.2 Cracker: Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se infiltra en un sistema

informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia. El cracker tiene como intención destruir. El cracker comete fraudes con tarjetas de crédito, por ejemplo, una persona posee una empresa que vende productos, esos productos pueden ser adquiridos vía web con el uso de una tarjeta de crédito, supongamos que entra un cracker y se apodera de los números de tarjetas de todas las personas que han comprado en ese sitio, el cracker usa la valiosa información que encontró en ese sitio, y piensa en cuanto puede vender esos números.

9.2.1 Armas de los crackers:

a) Cazadores de contraseñas.

Un cazador de contraseñas es un programa que desencripta las contraseñas o elimina su protección. Aunque estos programas no han de desencriptar nada, y además con determinados sistemas de encriptación es imposible invertir el proceso, si no es de forma autorizada. El funcionamiento es el siguiente: cogemos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización. Los cazadores de contraseñas que podemos encontrar son: Crack, CrackerJack, PaceCrak95, Qcrack, Pcrack, Hades, Star Cracker, etc. Hay cazadores de contraseñas para todos los sistemas operativos.

b) Caballos de Troya o troyanos:

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba

previsto, por. Ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos los crean los programadores, ya sea creando ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

c) Superzapping:

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serian las Pctools o el Norton Disk Editor.

d) Puertas falsas:

Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

9.2.2 Herramientas de destrucción de los crackers:

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocará el cuelgue del sistema. Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bombs, aplicaciones especiales de negación de servicio, y virus.

9.2.2.1 Mailbombing: Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario. Las herramientas que existen para estos ataques son: Up Yours, KaBoom, Avalanche, Unabomber, extreme mail, Homicide, Bombtrack, etc. La mayoría de estas aplicaciones suelen ser gratuitas, y tenemos para todas las plataformas.

9.2.2.2 Flash bombs: Son herramientas que se utilizan en el IRC. Cuando nos conectamos a un IRC, hay varios canales o chats, y cada chat tiene su operador que es la autoridad en ese chat, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bombs. Las aplicaciones de flahs bombs que existen atacan en el IRC de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal. Las herramientas que tenemos a nuestra disposición son: crash.irc, botkill2.irc, ACME, Saga, THUGS, o The 7th Sphere.

9.2.2.3 Aplicaciones de negación de servicios: Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina. Las utilidades que podemos encontrar para realizar este tipo de ataques son: Syn_floder, DNSKiller, arnudp100.c, cbcb.c, o win95ping.c.

9.2.2.4 Ataques asincrónicos: Este es quizá el procedimiento más complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

9.2.2.5 Ingeniería social: Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

9.2.2.6 Recogida de basura: Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos: el físico y el electrónico. El físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, p ej. El papel donde un operario apuntó su password y que tiró al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc. El electrónico, se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada, p. Ej. ficheros de swapping, ficheros borrados recuperables (por ejemplo, undelete), ficheros de spooling de impresora, etc.

9.2.2.7 Simulación de identidad: Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo desconectó y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

8.2.2.8 Spoofing: Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña. ¿Cómo se hace esto? Pues utilizando la dirección IP de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado. En máquinas UNIX se suelen utilizar para estos ataques los servicios "r", es decir, el rlogin y rsh; el primero facilita es procedimiento de registro en un ordenador remoto, y el segundo permite iniciar un shell en el ordenador remoto.

9.2.2.9 Sniffer: Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se

intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque mediante un sniffer se considera un riesgo muy alto, ¿por qué?, pues porque se pueden utilizar los sniffers para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a datos, no computadoras, y por ello es igual la plataforma que se utilice. Algunos sniffers son los siguientes: Gobbler, ETHLOAD, Netman, Esniff.c (se distribuye en código fuente), Sunsniff, linux_sniffer.c, etc.

9.3 Phreaker*:* hace una actividad parecida a la anterior, aunque ésta se realiza mediante líneas telefónicas y con y/o sin el auxilio de un equipo de cómputo. Es el especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

9.4 Virucker**:** Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

9.5 Pirata informático*:* Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor. ; hay que considerar también la piratería como descargar música de Internet y grabarla en un CD para escucharla; resulta pues que estamos

inmersos entre una juventud de "corsarios negros" y cada día hay programas donde se puede descargar gratuitamente el software para descargar la música gratuitamente[40].

10. Impacto de los delitos informáticos.

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 on-line 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 y el acecho.

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

[40]www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap5.htm

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 ganarle 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. Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes «infectados»; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas «descargados" de la red.

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 Barbara 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[41].

[41] www.mailxmail.com/curso/informatica/**delitos**informaticos/capitulo22.htm

CAPITULO III

TIPOS DE DELITOS INFORMÁTICOS MÁS COMUNES

1. Fraude a través de computadoras

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. Esta forma de realización se conoce como manipulación del input.

Ulrico Sieber[42], cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga -cómplice en la maniobra- mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

[42] Profesor titular de Derecho penal, Derecho de la información y Derecho informático, en la Universidad de München. www.jura.uni-muenchen.de/einrichtungen/ls/**sieber**/prof.htm

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor.

A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

Sieber cita como ejemplo el siguiente caso, tomado de la jurisprudencia alemana:
El autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor.

Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output.

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir,

cuantas veces quiera, la comisión del hecho. Incluso, en los casos de «manipulación del programa», la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active. En el ejemplo jurisprudencial citado al hacer referencia a las manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal. Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles Ej: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado » por el autor[43].

[43] www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo11.htm

2. - Conductas dirigidas a causar daños lógicos

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas 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. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se está trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» (cancer routine). En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

Una variante perfeccionada de la anterior modalidad es el «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los 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[44].

3. - La sustracción de información clasificada.

Se considera secreto industrial o comercial, toda información que guarde una persona con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros, en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas razonables para preservar su confidencialidad y el acceso restringido a la misma.
Ahora bien, para la protección de la información secreta, la ley de propiedad industrial de Nicaragua establece que toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios tenga acceso a un secreto a un secreto industrial o comercial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de utilizarlo para fines comerciales propios o de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado, en caso contrario será responsable de los daños y perjuicios ocasionados. También será responsable el que por medio ilícito obtenga información que contemple un secreto industrial o comercial[45].

---

[44] http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo10.htm

[45] www.mailxmail.com/curso/informatica/ delitosinformaticos/capitulo39.htm

4. Uso ilegítimo de sistemas informáticos ajenos.

Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometidas por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

Acceso no autorizado: La corriente reguladora sostiene 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[46].

5. El espionaje informático.

Una persona acostumbrada a navegar por la Red o utilizar correo electrónico ha podido ser víctima de espionaje, aunque en la mayoría de los casos, no se haya percatado de ello.

Bien, como sucede en todos los campos o materias de la vida, la tecnología avanza, y a pasos agigantados, lo que aporta grandes y notables beneficios a las comunicaciones y a la interacción de los distintos sectores de la economía. No obstante estos nuevos conocimientos pueden ser aprovechados por mentes maliciosas que los utilizan para fines menos éticos.

[46] http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo14.htm

La aparición en el mercado de nuevas técnicas y programas, difundidos en su mayor parte a través de Internet, posibilitan la recogida de información privada de un determinado usuario, sin dejar de mencionar aquellos programas que reconfiguran parámetros de los ordenadores aprovechándose del desconocimiento de las personas en el campo de las nuevas tecnologías[47].

Existen diferentes técnicas de espionaje informático, entre ellas:

- Dialers: está técnica consiste en la instalación de un marcador que provoca que la conexión a Internet se realice a través de un número de tarificación especial y no a través del nodo indicado por el operador con el que se haya contratado dicha conexión.
- Adware: se trata de programas que recogen o recopilan información a cerca de los hábitos de navegación del usuario en cuestión. Se suele utilizar con fines publicitarios para determinar qué, cómo, cuándo..., todo tipo de datos que indiquen la conducta de los internautas.
- Programas de acceso remoto: que permiten el acceso de un tercero a su ordenador para un posterior ataque o alteración de los datos. Son fácilmente reconocibles por los antivirus.
- Programas de espionaje o spyware: este tipo de programas basan su funcionamiento en registrar todo lo que se realiza en una PC, hasta un sencillo 'clic' en el ratón queda almacenado. Se utiliza para obtener información confidencial o conocer cuál es el funcionamiento que una persona le está dando a la máquina.

Como una muestra de lo real que puede ser la posibilidad de que pronto lleguemos a ser víctimas de espionaje informático, les relatamos la noticia que hace un par de meses apareció en Internet en el sitio de delitos informáticos, en el que se dio a conocer que una compañía estado-unidense, la "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.

[47] http://www.portaley.com/delitos-informaticos/espionaje.shtml

Según algunos expertos en seguridad informática, esta práctica parece violar la ley estadounidense.

Lo venden como una manera de poder saber que es lo que esta haciendo tu pareja, o cualquier otra persona cercana, como puede ser un hijo o similar. Su precio es de 89 dólares, y puede ser instalado hasta en cinco ordenadores.

Desde que el programa se instala, todas las acciones llevadas a cabo en el ordenador son registradas, desde un simple 'clic' de ratón. Esta información es posteriormente remitida a la persona que solicitó el servicio de espionaje.

No es este el único programa que sirve para espiar, hay otros como eBlaster de SpectorSoft, con la salvedad de que éste es instalado por el usuario en su propio ordenador[48].

6. La estafa informática.

6.1 El origen del término estafa.

La palabra "Estafa" contiene de forma inseparable el término "engaño" si bien se trata de un engaño de carácter económico, como señala el profesor Dr. Francisco Eugenio, la palabra estafa tiene un origen longobardo, es sinónimo de "estribo de montar a caballo", la expresión italiana "Staffare i piedi" quiere decir "sacar los pies del estribo" y por extensión, al que se estafa o tima, el que le engaña le deja económicamente en falso de modo análogo a como queda el jinete que ha sacado el pie del estribo.

6.2 Elementos de la estafa tradicional.

El vigente código penal vigente de España, al igual que nuestro código penal nicaragüense define la estafa del siguiente modo: "Cometen estafa los que con ánimo de lucro, utilizaren engaño bastante para producir error en otro,

[48] http.//www.maximail.com/delitosinformáticos/espionaje

induciéndole a realizar un acto de disposición en perjuicio propio o ajeno". Por tanto, son requisitos de la estafa, un engaño, un error que se produce en la víctima, un acto de disposición, un perjuicio para el autor del acto de disposición o para otra persona y un beneficio para el autor del engaño o también para otra persona.

6.3 Notas características de la estafa informática.

El auge de la informática en esta última década de siglo, introduciéndose de forma paulatina y persistente en todos los terrenos, hace que a medida que pasa el tiempo más y más aspectos de nuestra vida y entorno estén relacionados con ella, de todos esos aspectos, el patrimonial es uno de ellos y no el de menor importancia, no es de extrañar pues que nuestro patrimonio pueda sufrir ataques que utilicen como entorno la informática, de ahí que en el nuevo código penal español como respuesta a estos ataques se haya introducido en el Art.248, un segundo apartado que reza del siguiente modo: "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

Tres notas son de ver en esta nueva forma de estafa, en primer lugar la desaparición del requisito del engaño, en segundo lugar y como consecuencia de la primera nota, la desaparición también del error en la persona engañada, y a su vez como consecuencia de estas dos notas, el acercamiento (y hasta casi confusión) entre la estafa informática y el hurto.

6.4 La proximidad conceptual entre la estafa informática y el hurto.

Efectivamente, cabe plantearse la pregunta ¿Cuál es la verdadera naturaleza jurídica del hecho de la manipulación informática en provecho del activo patrimonial propio y en detrimento del activo patrimonial ajeno, es un hurto o

es una estafa?, por un lado tenemos que en la estafa informática no se ejerce violencia en las personas ni fuerza en las cosas, hay una manipulación informática y como consecuencia de ello, al igual que en el hurto, se produce una transferencia, una sustracción, un apoderamiento y finalmente, ese apoderamiento lo es de un bien mueble como es el dinero, si ese apoderamiento de dinero se produce sin el consentimiento de su dueño, ¿No podríamos estar ante un supuesto de delito de hurto?. Parece ser que la separación entre hurto y estafa producida por medios informáticos, viene determinada por el carácter material o inmaterial de la operación que genera la transferencia patrimonial de carácter ilícito, en el hurto, el objeto es una cosa corporal que materialmente toma el que lo comete, mientras que en la estafa informática se produce una manipulación informática irregular y que genera esa transferencia patrimonial, y así, la sustracción de una tarjeta de crédito del bolsillo de su dueño, sería un hurto y su posterior utilización por parte del sustractor para extraer dinero de un cajero automático sería una estafa informática, y ambas serían infracciones penales conexas.

6.5 Variedades más relevantes de la estafa informática

Veamos ahora algunas variedades de "estafa" o "hurto" informáticos referenciadas por los profesores de la UNED FRANCISCO EUGENIO Y EUGENIO OLIVER en su trabajo sobre Derecho informático:

6.4.1 Rounding of utility (redondeo): Es típico que se produzca un perjuicio de una multitud de titulares de cuentas en las que se producen en una secuencia temporal determinada, una o varias anotaciones fraudulentas por cantidades pequeñas redondeando por debajo en unas fracciones de unidad monetaria que resultan imperceptibles para el titular de una cuenta perjudicada, p.ej. una anotación de 19.774 córdobas. pasa a serlo de 19.770 tras la manipulación, al titular de la cuenta le puede pasar desapercibido este redondeo pero si se produce en una multitud de ellas y con regularidad, el beneficio del estafador puede ser considerable, estas operaciones, naturalmente se realizan con

ayuda de un programa de ordenador y del correspondiente equipamiento informático.

6.4.2. Data didling (Falsificación de datos): También mediante el oportuno programa de ordenador y correspondiente equipamiento informático se cambia la información de modo que las operaciones de ingreso de dinero en una cuenta van a parar a otra o las operaciones de salida de dinero se cargan a otra cuenta distinta de la del receptor, como consecuencia de ello, hay un incremento en el patrimonio de una persona a costa de un detrimento del patrimonio de otra.

6.4.3 Piggy backing (suplantación de la personalidad del usuario): También mediante la utilización inteligente y fraudulenta de equipos y programas informáticos se produce acceso, una invasión, a cierta información que acaba siendo utilizada en favor del "invasor" mediante sustracciones de dinero o signos que lo representan y en detrimento del dinero, o, es lo mismo, los signos representativos de dinero, que hay en el sistema informático invadido y del que se realiza la oportuna y sofisticada sustracción[49].

7. La falsificación informática.

7.1 ¿Qué es la falsificación informática?

A este tipo de conducta criminal, se lo conoce como "Falsedad Vía Computarizada, porque a través de la misma, se pueden elaborar tarjetas de crédito, cheques, títulos valores, en general todo tipo de documentos públicos y privados, o se pueden alterar todo el sistema contable de una Empresa, facilitando a las Sociedades Comerciales llevar la doble contabilidad, todo esto con miras a evadir impuestos"

[49] http://www.alfa-redi.org/rdi-articulo.shtml?x=212

En este caso, el sujeto se vale de computadores, impresoras láser, scanner y demás accesorios de alta tecnología para elaborar documentos, reproducir nuevos tamaños, buscar estilos de letras o crear logotipos, que años atrás se podían hacer únicamente utilizando equipos sofisticados[50].

7.2 Características de la falsificación informática.

7.2.1 Este delito es eminentemente doloso, porque en el actor hay voluntad de delinquir. Y logra su objetivo utilizando la computadora para alterar o modificar mensajes de datos o cualquier información.

7.2.2 Al igual que muchos otros delitos informáticos, este es un delito de cuello blanco (white collar) porque los hechos punibles los cometen únicamente determinadas personas que necesitan cierta preparación y conocimientos específicos, lo que exige que sean personas de apreciable nivel cultural y económico. En algunos casos son estudiantes que operan ya desde sus lugares de enseñanza o capacitación, o bien desde sus hogares, cuando disponen de computadoras personales.

7.2.3 Buscan el momento propicio para ejecutarlas. Algunos autores lo llaman "*deshonestidad latente del criminal informático"* porque esperan que la proporción de ganancia sea alta para correr con los riesgos que implica una falsificación.

7.2.4 Son acciones que se pueden consumar en milésimas de segundo.

7.2.5 Estas acciones provocan serias pérdidas económicas.

7.2.6 Son delitos de constante aumento o crecimiento y pocas denuncias, lo que hace que las autoridades por no conocerlos, no los investiguen, haciendo parte de lo que criminológicamente se conoce como la "*cifra*

[50] Según Dra. María Cristina Vallejo, Abogada y especialista superior en derecho financiero y bursátil.(http://www.dlh.lahora.com)

oscura" o dorada, porque sus autores pertenecen a círculos sociales altos[51].

8. El sabotaje informático.

8.1 – Concepto de sabotaje informático.

El Sabotaje informático doctrinariamente, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.

El acceder sin ser autorizados a servicios y sistemas informáticos que van desde la simple curiosidad, como es el caso de los piratas informáticos (hackers), hasta el sabotaje informático.

Este delito, puede entrañar una perdida económica sustancial para los propietarios legítimos de Empresas, Instituciones públicas, privadas, Gubernamentales, etc.

El Sabotaje o Daño Informático puede tener lugar en Internet en dos formas: a.- Puede producirse por medio de la modificación y/o destrucción de los datos o programas del sistema infectado, o b.- puede producirse por medio de la paralización o bloqueo del sistema, sin que necesariamente se produzca alteración ni destrucción de los datos o programas.

Es oportuno indicar, que legislaciones a nivel mundial han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. Como muestra de ello, citamos el artículo 415 del código penal de Ecuador que tipifica este delito como "Daño Informático", imponiendo una prisión de 6 meses a 3 años y multa de 60 a 150 dólares para aquél que en forma maliciosa, destruya, altere, suprima o inutilice programas, bases de datos o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena de 3 a 5 años y multa de 200 a 600 Dólares en caso de que afectare datos contenidos en las

[51] http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.31.htm

computadoras o en el sistema de redes destinado a prestar un servicio público o que tengan que ver con la Defensa Nacional.

El sabotaje informático, es llevado a cabo, en la mayoría de los casos por empleados descontentos y puede producirse, tanto a la parte física del ordenador (hardware) como a la parte lógica del mismo (software). Los daños al software se pueden causar a través de elementos electromagnéticos, cuyas técnicas son las siguientes: la introducción de virus, gusanos o una bomba lógica que destruye, altere o inutilice los programas, datos o documentos electrónicos almacenados en el sistema informático.

8.2 – Modalidades más conocidas del sabotaje informático.

8.2.1 Los virus informáticos. Son una serie de instrucciones de programación que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar al sistema por conducto de un soporte lógico (floppy, CD-ROM, etc) que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Los Virus informáticos se esconden en los dispositivos de almacenamiento y si en estos se encuentran otros programas o datos son contaminados en ese momento por aquellos. Ningún programa de Virus puede funcionar por si sólo, requiere de otros programas para poderlos corromper. Su otra característica es la capacidad que tienen de auto duplicación, haciendo copias iguales de sí mismos, entrando furtivamente y provocando anomalías en las computadoras al desarrollar su función destructora. Se les ha dado el nombre de Virus por la analogía que tiene su comportamiento con el de los Virus Biológicos.

8.2.2 – Los gusanos informáticos: Son aquellos que se fabrican de forma lógica al virus y su intención es infiltrarse en programa de procesamientos de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse, por lo tanto no es tan grave como el virus. Tratan de

reproducirse a si mismos. No tienen efectos destructivos pero colapsan la memoria del sistema o el ancho de banda simplemente aumentando su número rápidamente[52].

8.2.3 – Las bombas lógicas: Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario. Realizarlas exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos. Es importante destacar, que a diferencia de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; es por esta razón, que de todos los dispositivos informáticos criminales, la bomba lógica es la que más daño hace dentro del sistema informático. Es difícil saber cuál es el sujeto, por cuanto se puede programar la detonación para que tenga lugar mucho tiempo después de que se haya marchado el criminal informático[53].

La delincuencia cibernética, generalmente se basa en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente en Países donde la tecnología está más avanzada y en otros donde se está desarrollando notablemente, conlleva también a la posibilidad creciente de estos delitos[54].

9. La piratería informática.

Muchas empresas y organizaciones no son conscientes de que quizá estén usando software ilegal. La distribución y uso ilegales del software constituyen un problema importante que afecta negativamente a los proveedores de software.

[52] http://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico
[53] http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node77.html
[54] www.proasetel.com/paginas/articulos/**sabotaje**_informatico.htm

La piratería informática es un gran problema. Las cifras de Business Software Alliance[55] indican que el sector pierde casi 29.000 millones de dólares anuales a causa de la piratería informática. Traducido a porcentajes, el 35% de las aplicaciones usadas en las empresas (más de una de cada tres), son ilegales.

La piratería informática consiste en la distribución o reproducción ilegal de software. Comprar software significa en realidad comprar una licencia para usar el software, y esta licencia especifica la forma legal de usar dicho software. Cualquier uso que se haga del software más allá de lo estipulado en la licencia constituye una violación de ésta y posiblemente, de las leyes que amparan los derechos de propiedad intelectual. La piratería informática es ilegal y sancionable según la ley, tanto si es deliberada como si no.

9.1 Formas de piratería informática:

La piratería informática adopta muchas formas. Aquí tenemos algunas de ellas:

9.1.1 Usuarios de empresa o usuarios finales:

- informar de un número inferior al real de las instalaciones de software adquiridas mediante acuerdos de compra de gran volumen,.
- Hacer copias adicionales del software sin tener el número de licencias necesario para ello; por ejemplo, se dispone de 1 copia con licencia, pero se hacen cinco copias adicionales.
- Servidor: instalar el software en un servidor al que todo el personal tiene acceso ilimitado (sin mecanismos de bloqueo, contadores, etc.).

9.1.2 Licencias de suscripción: usar software de licencia de suscripción más allá de la fecha de vencimiento.

[55] Es una organización dedicada a promover el uso seguro y legal de los productos de software.

9.1.3 Derecho a PrimeSupport: acceso al derecho a PrimeSupport (por ejemplo, archivos DAT, SuperDAT, actualizaciones o nuevas versiones) sin disponer de un acuerdo PrimeSupport vigente y válido.

9.1.4 Piratería por Internet: puede adoptar muchos aspectos diferentes. Entre ellos:

- Dar acceso al software, generador de claves, claves de activación, números de serie y similar que permitan instalar el software, mediante descarga, desde CD grabados o desde el soporte original.
    i. El proveedor ofrece una copia; no se pueden distribuir las copias de seguridad.
    ii. El producto ofrecido ha sido distribuido previamente infringiendo un contrato de distribuidor, reseller, contrato académico u otro tipo de contrato.
    iii. El producto ofrecido ha sido usado previamente para obtener la actualización a una versión más reciente.
    iv. El producto es una versión beta o no publicada.
- Se facilitan enlaces a herramientas, o se distribuyen herramientas, que subvierten o socavan las protecciones contra copia o las funciones de agotamiento de plazo del software.

9.1.5 Falsificación: cuando se intenta copiar el producto y su presentación de forma que parezca original.

9.1.6 Carga en el disco duro: es el caso de ciertos proveedores poco escrupulosos que instalan software ilegalmente para vender mejor sus equipos. Si bien son muchos los proveedores autorizados a instalar productos en los equipos que venden, los proveedores honrados suministran el software mediante acuerdos con los proveedores de dicho software.

En Estados Unidos la consecuencia de la piratería informática puede ser el arresto y enjuiciamiento criminal del infractor, con indemnizaciones de hasta 250.000 dólares y penas de prisión de hasta cinco años. En los casos civiles, la parte demandante tiene derecho a percibir el importe más alto entre la suma de su pérdida de beneficios más los beneficios del infractor y los daños que establece la ley, a razón de 150.000 dólares por producto. Además, la parte actora puede procurar recuperar los honorarios de sus abogados[56].

10. La pornografía infantil en Internet.

Este no es uno de los delitos meramente informático, ya sea por el fin o por el bien jurídico protegido, por que en realidad lo que se protege en él, es la indemnidad sexual del menor, pero resulta de sumo interés el que su comisión haya aumentado con la aparición de los medios informáticos, y que con esta característica plantee también retos doctrinarios y legislativos, como lo hacen los otros delitos informáticos.

La pornografía infantil constituye un problema de dimensión internacional, que se ha amplificado con la irrupción de nuevas tecnologías que han transformado las pautas de producción y difusión de este tipo de material. La transformación de la producción y difusión de la pornografía infantil en general, y particularmente aprovechando el nuevo escenario que facilitan las nuevas tecnologías, abre interrogantes al Derecho Penal de diversa consideración. De una parte, la transnacionalidad del fenómeno obliga a buscar consenso sobre las necesidades de tutela, concretamente en aspectos como la tipificación de la denominada pornografía infantil virtual, la pornografía pseudoinfantil, la posesión para el consumo o, en último término, la edad de los menores. En este debate debe situarse asimismo la polémica sobre la responsabilidad de los intermediarios.

[56] http://www.mcafee.com/es/antipiracy_policy.htm

La Convención de las Naciones Unidas sobre los Derechos del Niño (UNCRC), que ha sido mayoritariamente ratificada por los estados, califica la pornografía infantil como una violación de los derechos del menor y exige a las naciones que participen en la convención internacional y que adopten medidas para prevenir la explotación infantil en materiales de tipo pornográfico (Art. 34). Asimismo, el Programa de acción para la prevención de la venta de niños, prostitución infantil y pornografía infantil de la Comisión Pro Derechos Humanos de las Naciones Unidas respalda los esfuerzos internacionales y de la Comisión en cuanto a la represión y castigo de conductas de explotación de los menores con fines pornográficos. No obstante, las acciones internacionales de lucha contra la explotación sexual de los menores y contra la producción y el tráfico de la pornografía infantil encuentran serios escollos de partida[57].

10.1 Definición de pornografía infantil.

La definición de pornografía infantil depende de múltiples factores de tipo cultural, de creencias de tipo moral, de pautas de comportamiento sexual, así como de las ideas religiosas imperantes en cada comunidad. Lógicamente, estas fluctuaciones conceptuales tienen un reflejo en los conceptos legales utilizados por los ordenamientos de cada país. Estos factores explican que tampoco existan convenciones jurídicas internacionalmente uniformes en torno al límite legal a partir del cual se acota el concepto de niño o de menor.

La UNCRC[58] define al niño como persona menor de 18 años, y ésta es la convención normativa imperante en el contexto jurídico y cultural del continente europeo. Por el contrario, en países como Australia, la legislación sobre pornografía infantil conceptúa al niño como menor de 16 años, mientras que en algunas jurisdicciones de los Estados Unidos (EE.UU.) los menores a partir de los 15 años pueden consentir legalmente en orden a mantener relaciones sexuales

[57] www.solocursos.net/pornografia_ **infantil**_e_internet-slccurso1110235.htm
[58] La Convención de las Naciones Unidas sobre los Derechos del Niño.

con un adulto; sin embargo, conforme a la legislación de esos propios estados de EE.UU., ese adulto no puede elaborar, producir, distribuir ni tan siquiera poseer una filmación o registro visual de sus contactos sexuales con el menor, de acuerdo con los Estatutos Federales de Pornografía Infantil, por cuanto éstos definen al menor como persona que no ha cumplido los 18 años. Pese a todos estos obstáculos de partida, el Consejo de Europa define la pornografía infantil como "cualquier material audiovisual que utiliza niños en un contexto sexual".

10.2 El desarrollo histórico de la difusión de la pornografía infantil por Internet.

En la década de los años setenta puede situarse el momento de máximo apogeo de la producción comercial de pornografía infantil en el mundo occidental. En aquellos años Dinamarca, Holanda y Suecia constituían los principales centros de producción. A finales de dicha década y comienzos de los años ochenta se verifica una mayor intervención gubernamental y el impulso de medidas legislativas, centradas en la prohibición de la producción, la venta y la distribución de la pornografía infantil.

En los años noventa se ha acrecentado la adopción de medidas legislativas prohibitivas y el impulso de la represión penal sobre las actividades de producción, difusión, exhibición y distribución de material pornográfico infantil al compás de la evolución tecnológica, y no faltan además muestras de una "nueva cruzada legislativa" en la que incluso se opta por la incriminación de la mera tenencia o posesión de material pornográfico infantil. En la actualidad se constata una tendencia según la cual el tráfico de pornografía infantil no viene presidido por el ánimo de lucro ni por motivos comerciales. Se ha acrecentado así el intercambio de material entre pedófilos, pauta de comportamiento que se ha amplificado en las nuevas autopistas de la información (Internet), donde los usuarios pueden introducir material y convertirse en difusores de dicho material. Por consiguiente, puede trazarse una línea evolutiva que desplaza la elaboración y producción de la pornografía infantil de parámetros comerciales organizados a ámbitos

descentralizados amateurs y domésticos. A esta evolución ha contribuido también el denominado "turismo sexual", pues se ha constatado en los últimos tiempos que una buena parte de la elaboración de material pornográfico infantil tiene su origen en filmaciones amateurs llevadas a cabo por turistas que entablan relaciones con menores, principalmente en países del continente asiático.

En efecto, esta evolución no hubiera sido posible sin la masificación y el abaratamiento de los aparatos de vídeo doméstico. Estas líneas evolutivas se han agudizado con la irrupción de Internet como nueva autopista de la información. Puede indicarse, pues, que la tecnología informática ha acabado por consolidar las pautas y patrones de la producción y el tráfico de pornografía infantil. Cualquier usuario de la Red tiene acceso a los servicios en línea en una autopista de información a la que se encuentran conectados más de 30 millones de personas.

En este contexto, cualquier usuario puede erigirse en productor, difusor o receptor de material pornográfico infantil.

Por último, la evolución de la informática permite la alteración de imágenes por ordenador, de modo que se puede enmascarar la imagen de adultos que participan en actos pornográficos o de contenido sexual para que parezcan menores de edad; se trata de la denominada pornografía técnica. Este tipo de pornografía presenta una menor lesividad en la medida que no utiliza menores reales en la elaboración del material. Conceptualmente diversa en la pseudopornografía de menores, consistente en la alteración de imágenes por medio de la colocación de la cara de un menor sobre la imagen de un adulto o bien en el añadido de objetos a una imagen; en tales casos, siempre que se incorporen, aunque sea parcialmente, imágenes de menores reales, la lesividad de la conducta es mayor y probablemente debe ser objeto de sanción penal.

El tráfico de pornografía infantil en Internet ha sido objeto de recientes encuentros internacionales de expertos, como el celebrado en Lyón en mayo de 1998. En este

congreso, los representantes de 19 países y organizaciones no gubernamentales, implantadas en el sector, efectuaron, entre otras, las siguientes recomendaciones: a) la necesidad de adopción en la legislación de los ordenamientos nacionales de medidas legislativas que incriminen la producción, distribución, comunicación, importación, exportación y posesión de pornografía infantil, incluida la pseudo-pornografía, a través de Internet; b) la armonización internacional en cuanto al límite de edad en la conceptualización de los menores y en cuanto a la definición de pornografía infantil; c) el incremento de la cooperación policial y judicial, tanto en cuestiones relativas a la aplicación de la ley penal como con relación a la asistencia técnica; d) la solicitud a las Naciones Unidas de que impulse un borrador de legislación tipo, uniforme, contra la pornografía infantil; e) la solicitud al Comité sobre Derechos de los Niños de las Naciones Unidas de que impulse la aplicación de controles legales adecuados contra la pornografía infantil, cuando los gobiernos presenten sus informes nacionales en la Convención sobre

Derechos del Niño; f) la promoción del desarrollo de programas similares a los antivirus, que permitan filtrar o bloquear la pornografía infantil en Internet, a través de los proveedores de servicio en Internet (PSI), mediante una base de datos central actualizada regularmente con impresiones de imágenes de pornografía infantil[59].

10.3 El tráfico de la pornografía infantil y sus problemas jurídicos.

La Red ha nacido bajo los designios de la anomia jurídica. No existe un estatuto jurídico sobre Internet. Puede indicarse que la ausencia de regulación jurídica, de límites y de control sobre los flujos de información son algunas de las notas características básicas de esta autopista de la información. Como señala Morón Lerma: "Internet no tiene presidente, director ejecutivo o mandatario. No existe la figura de una autoridad máxima como un todo. En realidad, nadie gobierna Internet, no existe una entidad que diga la última palabra. No está bajo el control

[59] Fermín Morales, catedrático de Derecho penal de la Universidad de Barcelona.

de ninguna empresa y, de hecho, son los propios usuarios quienes asumen la responsabilidad de su funcionamiento. Cada red integrante de Internet tiene sus propias reglas". En este contexto, puede comprenderse con prontitud que los problemas principales de la efectividad de la represión penal del tráfico de pornografía infantil en la red no dependen exclusivamente de la tipificación de conductas en los códigos penales, sino de la propia lógica de funcionamiento de Internet y de la dimensión internacional de las conductas ilícitas a sancionar penalmente. La Red se ha desarrollado y consolidado como nueva autopista de la información de masas bajo la lógica de la libertad de información o del libre flujo de la información.

En este sentido, el intervencionismo estatal ha sido considerado como un factor que podría llegar a poner en peligro Internet; de ahí que en la nueva sociedad de la información se enarbolen estandartes anti-estatalitas y se postulen soluciones cifradas en la autorregulación de los operadores en la Red, siempre al margen de regulaciones jurídicas heterónomas impuestas por los estados o por los organismos internacionales a través de tratados o convenios internacionales.

Sin embargo, en la actualidad se va consolidando la idea de que las reglas en la Red no pueden quedar al albur exclusivo de los usuarios. El magma de intereses contrapuestos en Internet (derecho al anonimato del usuario, garantía de la confidencialidad de comunicaciones personales en la Red, confianza y seguridad jurídica en el mercado virtual, preservación de la seguridad y defensa de los estados...) exige nuevas soluciones jurídicas complejas, que atiendan al principio de proporcionalidad, en el buen entendido de que se trata mediante el mismo de garantizar la convivencia y preservación simultánea de intereses legítimos en tensión. Y el problema exige que sean descartadas soluciones simplistas que superen las esquemáticas dicotomías "liberalización contra control" o "estados contra usuarios". Más particularmente, la transmisión de contenidos ilícitos o nocivos en la Red, como por los relativos a difusión de pornografía infantil, suscitan la imperiosa necesidad de soluciones jurídicas que permitan conjugar la

libertad de información con la preservación de otros intereses, en el caso analizado los intereses del menor, cifrados en el derecho a la propia imagen del mismo, conectado con el derecho a la privacidad, aspectos todos ellos íntimamente ligados con la dignidad humana y libre desarrollo de la personalidad del menor.

No obstante, como antes se ha apuntado, la dimensión internacional de Internet y sus específicas connotaciones (uso masivo, descentralización, automatismo etc.) suponen serios obstáculos a la hora de afrontar propuestas de solución jurídica. Una cuestión parece clara: el estatuto jurídico de Internet no puede ser abordado desde una perspectiva nacional. Una política jurídica de futuro, tendente a elucidar el gobierno jurídico de la Red y en su seno la determinación de la esfera de responsabilidad jurídica, exige soluciones de carácter internacional. Durante un primer periodo en el ámbito europeo se han fomentado códigos o convenios de autorregulación en Internet; a este designio responde la Resolución del Consejo de la Unión Europea, de 17 de febrero de 1997 (DOC, núm. 70, de 6 de marzo), sobre contenidos ilícitos en Internet.

En la referida resolución se insta a los estados miembros a "estimular y favorecer sistemas de autorregulación que incluyan organismos representativos de los proveedores de servicios y de los usuarios de Internet". Esta resolución constituyó el punto de partida del informe provisional sobre las iniciativas emprendidas por los estados de la Unión Europea contra los contenidos ilícitos y nocivos en la Red. Los primeros pasos de la Unión Europea se encaminan a subrayar: a) la inconveniencia de que en el futuro reine la anomia en Internet; b) la necesidad de introducir una regulación jurídica armoniosa con la lógica de funcionamiento de Internet, con especial énfasis en que la introducción exclusiva de normas represivas podría perjudicar el desarrollo de la Red; c) la necesidad de caminar hacia una paulatina armonización de los ordenamientos nacionales.

La complejidad de problemas jurídicos que suscita la Red viene dada por el dato de que cada usuario, conectado a la misma, puede erigirse en difusor de contenidos por distintas vías, tales como el correo electrónico, introducción de boletines, participación en foros de discusión o introducción de páginas web. Esta posibilidad de introducción de mensajes o contenidos en la Red, de forma masificada y difusa, constituye uno de los factores que convierten en dificultosa la persecución de la difusión de pornografía infantil en la Red, dificultad que afecta a lo probatorio y, en particular, a la identificación de los autores de las conductas de tal tráfico ilícito.

En los foros de discusión se alude a contenidos ilícitos y nocivos en Internet como si de un mismo problema se tratase, cuando en realidad se trata de dos categorías conceptuales de contenidos diversos. Las medidas jurídicas de respuesta a la difusión de contenidos ilícitos, entre ellos el tráfico de pornografía infantil, reclaman respuestas jurídicas puntuales enderezadas a sancionar la fuente originaria de tal difusión. Por el contrario, los contenidos nocivos constituyen un concepto más difuso, que alude a la necesidad de generar pautas culturales en la red tendentes a sensibilizar a los usuarios, para lograr así la paulatina erradicación de aquellos. La instauración de reglas jurídicas firmes en Internet, orientada a un férreo control sobre los contenidos que circulan en ella, constituye una apuesta quimérica. No sólo porque, como se ha dicho, la Red se articula de manera descentralizada, sino también porque el material que incorpora contenido ilícito puede ser ubicado con rapidez en otro servidor "de pantalla", con el fin de evitar la persecución del delito.

En definitiva, es preciso avanzar hacia normas de armonización internacional comunes, por medio de tratados internacionales que deberán quedar complementados con medidas de cooperación internacional de tipo judicial y policial. Asimismo, deberá prestarse atención a los avances técnicos para poder perfilar en el futuro un estatuto jurídico más penetrante sobre la responsabilidad de los proveedores, tendente a exigir un mayor y escalonado control sobre la

información ilícita que circula en la Red. Éstos son los presupuestos político-criminales para una racional y efectiva represión penal del tráfico de pornografía infantil en la Red[60].

En el código penal nicaragüense no se hace ninguna referencia directa al término "Pornografía infantil", pero tal acción no quedaría impune por resultar aplicable el artículo 201 Pn. que habla de la corrupción de menores, incluso se tipificaría como corrupción de menores agravada por el inciso 2) que habla del propósito de lucro o de satisfacer deseo de terceros.

11. El terrorismo en Internet.

Este es otro delito que no calificaremos como informático por su esencia, o sea por el fin o por que su comisión afecta la información como bien jurídico, sino que más bien adquiere la calidad de informático por el uso de la red para desarrollarse, en otras palabras decimos que el terrorismo nos interesa aquí señalarlo por que actualmente sus adeptos lo ejercen echando mano de las ventajas que ofrece la informática y la red internacional (Internet).

Aunque se debate con frecuencia el peligro que el ciberterrorismo representa para Internet, es sorprendente el escaso conocimiento sobre la amenaza que plantea el uso de la red por parte de los terroristas. Un reciente estudio realizado a lo largo de seis años pone de manifiesto que las organizaciones terroristas y sus partidarios han utilizado todas las herramientas que ofrece Internet para reclutar adeptos, recaudar fondos y lanzar una campaña de intimidación a escala mundial. También muestra con claridad que para combatir de modo eficaz el terrorismo no basta con la mera supresión de sus herramientas de Internet[61].

[60] http://www.uoc.edu/in3/dt/20056/

[61] Investigación hecha por GABRIEL WEIMANN, investigador del United States Institute of Peace y profesor de Comunicación de la Universidad de Haifa (Israell).

.

Se ha definido a menudo el terrorismo como una forma de guerra psicológica y no hay duda de que los terroristas han tratado de librar semejante guerra a través de Internet. Existen incontables ejemplos sobre cómo se sirven de este medio sin censura para propagar desinformación, realizar amenazas que pretenden infundir miedo y sensación de indefensión, así como divulgar espantosas imágenes de sus acciones recientes. Desde el 11 de septiembre del 2001, Al Qaeda ha llenado su sede web con una sarta de anuncios sobre un inminente "ataque a gran escala" contra objetivos estadounidenses. Tales advertencias han recibido una considerable cobertura por parte de los medios de comunicación, lo que ha contribuido a crear un sentimiento generalizado de temor e inseguridad en la opinión pública de todo el mundo y, sobre todo, en Estados Unidos. Es interesante constatar que Al Qaeda ha proclamado de manera sistemática en sus sedes que la destrucción del World Trade Center ha infligido daños psicológicos, además de materiales, a la economía estadounidense.

Internet ha ampliado significativamente las posibilidades de conseguir publicidad por parte de los grupos terroristas. Antes de la llegada de Internet, las esperanzas de conseguir publicidad para sus causas y acciones dependían de lograr la atención de la televisión, la radio y la prensa. Ahora, el hecho de que los propios terroristas controlen de manera directa el contenido de sus sedes les proporciona mayores posibilidades de influenciar el modo en que son percibidos por distintos tipos de público objetivo y manipular su imagen y las de sus enemigos.

La mayoría de las sedes de terroristas no ensalzan las acciones violentas. Más bien –y con independencia de su naturaleza, móviles y ubicación geográfica–, ponen énfasis en dos temas: las restricciones que sufre la libertad de expresión y la difícil situación de sus camaradas convertidos ahora en prisioneros políticos.

Ambos temas tienen un amplio predicamento entre sus propios partidarios y tienen también el propósito de despertar la simpatía del público occidental que aprecia la libertad de expresión y desaprueba las medidas que silencian la oposición política. La sede de la secta japonesa de la Verdad Suprema (Aum-Shinrikyo) ilustra bien

el espíritu liberal de la ciberpropaganda terrorista. En 1995, algunos integrantes de la secta realizaron un atentado mortal con gas sarín en el metro de Tokio que costó la vida de 12 personas e intoxicó a otras 5.000. Su nueva sede en Internet es muy sofisticada y atractiva. Un diseño azulado de estilo nueva era –con relajantes aguas y el símbolo de la paloma de la paz– domina la página principal y complementa su título: “Liberación del alma, la era de la benevolencia”.

Los terroristas no sólo han demostrado tener mucha habilidad para el marketing en línea, sino también ser expertos en recopilar información de los más de mil millones de sedes que forman la telaraña mundial. Por medio de Internet pueden averiguar los horarios y la localización de objetivos tales como servicios de transporte, centrales nucleares, edificios públicos, aeropuertos y puertos, así como las medidas antiterroristas.

Además de solicitar en línea ayuda financiera, los terroristas reclutan activistas usando toda la gama de tecnologías web (audio, vídeo digital, etcétera) destinadas a realzar la presentación de sus mensajes. Y, del mismo modo que las sedes comerciales rastrean a los visitantes para elaborar perfiles de consumo, las organizaciones terroristas reúnen información sobre los usuarios que navegan por sus sedes. Luego contactan a aquellos visitantes que parecen más interesados en la organización o más apropiados para trabajar en ella. Los encargados del reclutamiento pueden usar también tecnologías más interactivas para pasear en línea por salas de charla y cibercafés con el fin de buscar personas receptivas entre el público, en particular jóvenes. El Instituto SITE, un grupo de investigación radicado en Washington que vigila las comunicaciones de Al Qaeda por Internet, ha proporcionado estremecedores pormenores sobre una sofisticada oleada lanzada en el 2003 para reclutar combatientes dispuestos a viajar a Irak para combatir a las fuerzas estadounidenses y de la coalición.

Además, Internet proporciona a los terroristas medios baratos y eficaces de interconexión. A través de Internet, estos grupos interconectados de manera flexible son capaces de mantener relaciones con sus propios integrantes y con

miembros de otros grupos terroristas. Internet no solo conecta a los militantes de una misma organización terrorista, sino también a los militantes de distintos grupos. Decenas de sedes que apoyan el terrorismo en nombre de la "yihad", por ejemplo, hacen posible que terroristas situados en lugares tan distantes como Chechenia y Malasia intercambien ideas e información práctica sobre cómo fabricar bombas, establecer células terroristas y realizar ataques. Otro ejemplo es el "Manual de venenos de los mujaidines", que se distribuye ampliamente en línea y ofrece minuciosas instrucciones sobre cómo fabricar diversas armas.

Los terroristas utilizan Internet no sólo para aprender a fabricar bombas, sino también para planear y coordinar ataques específicos. Los miembros de Al Qaeda dependían en gran parte de Internet al planear y coordinar los ataques del 11-S.

En el ordenador de Abu Zubayda, terrorista de Al Qaeda detenido y del que se dice que habría sido el cerebro de los atentados, los agentes federales encontraron miles de mensajes codificados sacados de una parte de una sede web protegida con una contraseña[62].

[62] http://yaleglobal.yale.edu/display.article?id=4029

CAPITULO IV.

LEGISLACIÓN NACIONAL E INTERNACIONAL SOBRE DELITOS INFORMÁTICOS.

1. La Xl convención de las Naciones unidas sobre justicia penal y prevención de delitos.

El undécimo Congreso de las Naciones Unidas sobre Prevención del Crimen y Justicia Penal concluyó en Tailandia con la adopción de la Declaración de Bangkok, un documento que insta a actuar contra el crimen organizado y el terrorismo. El texto cubre una serie de temas, como el tráfico de personas, el lavado de dinero, la corrupción, y los delitos cibernéticos. Reconoce que las estrategias amplias de prevención podrían reducir estos crímenes, pero advierte que para lograrlo dichas tácticas tienen que abordar las causas radicales y los factores de riesgo del crimen y la victimización. En la Declaración los países también refrendan su compromiso de cooperación internacional en la lucha contra el crimen y el terrorismo a nivel multilateral, regional y bilateral en áreas que incluyen la extradición y asistencia legal mutua. Además, el documento pide a la comunidad internacional que ayude a los países que están emergiendo en conflictos armados para que restablezcan y fortalezcan el estado de derecho y puedan impartir justicia[63].

2. La convención europea sobre los delitos informáticos.

El pasado 23 de noviembre del 2001, el Consejo de Ministros de Europa, compuesto por los Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón firmaron en Budapest la Convención sobre Delitos Informáticos.

[63] http://www.cinu.org.mx/11congreso/UN/prensa.htm

Esta Convención, cuya elaboración tomó más de cuatro años, tuvo como objetivos fundamentales los siguientes: 1) Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; 2) Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y 3) Establecer un régimen dinámico y efectivo de cooperación internacional.

La estructura normativa de este novedoso instrumento jurídico internacional consta de 4 capítulos. El capítulo I define algunos conceptos básicos, tales como "sistema de cómputo", "datos informáticos", "proveedor de servicios de interconexión o almacenamiento de datos informáticos" e "intercambio electrónico de datos". El capítulo II establece las medidas que deben adoptar los Estados signatarios dentro del marco de sus legislaciones penales sustantivas (sección 1) y adjetivas (sección 2). Por último, el capítulo III recoge los principios generales de cooperación internacional, incluyendo aspectos tales como extradición, asistencia legal mutua e intercambio de información.

La sección 1 del Capítulo II está dividida, a su vez, en cinco títulos que establecen nuevas categorías penales sobre conductas asociadas con el almacenamiento, tratamiento y transmisión ilegítima e intencional de datos a través sistemas de cómputo (hardware) y programas informáticos (software).

El título 1 describe dentro de los "Delitos contra la Confidencialidad, Integridad y Disponibilidad de Datos y Sistemas de Cómputo" a los siguientes actos: "Acceso ilegal", que comprende la interceptación e interferencia ilegal de datos y sistemas de cómputo, conocido también como "hacking" y el "uso inapropiado de programas informáticos y sistemas de cómputo", que contempla el sabotaje y daños ocasionados a equipos informáticos, comúnmente denominado "cracking".

Por su parte, el título 2 contempla los "Delitos relacionados con Sistemas de Cómputo" y los "Delitos relacionados con el Contenido de los Datos Informáticos", entre los que destacan las siguientes conductas delictivas: Alteración, supresión y eliminación de datos informáticos y fraude informático (entendiéndose como tal "todo acto ilegítimo e intencional que ocasione la pérdida de patrimonio, cometido a través de la alteración, supresión, eliminación e interferencia de datos informáticos o sistemas de cómputo).

El título 3 establece los "Delitos relacionados con el contenido de los Datos Informáticos". Dentro de esta categoría se encuentran las siguientes formas de comportamiento antisocial: Producción, ofrecimiento, distribución y posesión de Pornografía Infantil. El concepto de pornografía infantil, de acuerdo con el artículo 9.2 de la Convención, abarca todo material pornográfico que visualmente evidencie lo siguiente: (1) Un menor de edad envuelto en conducta sexual explícita, (2) Una persona que aparente ser menor de edad envuelta en conducta sexual explícita, (3) Imágenes realistas que representen a un menor de edad envuelto en conducta sexual explícita. El término menor de edad hace alusión a los menores de 18 años; no obstante, la Convención admite que los Estados firmantes reconozcan un límite de edad inferior, siempre y cuando no sea menor a los 16 años.

El título 4 regula los "Delitos relacionados con la Violación de los Derechos de Autor", reconociendo la necesidad de dar validez a los acuerdos internacionales sobre esta materia, entre otros, la Convención de Berna para la Protección de Trabajos Literarios y Artísticos, el Acuerdo de la OMC sobre Aspectos de Comercio Relacionados con la Propiedad Intelectual, y el Tratado sobre Derechos de Autor de la Organización Mundial de la Propiedad Intelectual (OMPI).

Por último, el título 5 establece un régimen de responsabilidad penal para las personas jurídicas que estén involucradas en alguna de las conductas descritas en los primeros cuatro títulos. Así, en su artículo 12, la Convención señala que "cada

Estado parte deberá adoptar las medidas legislativas que sean necesarias para asegurar que las personas jurídicas sean responsables penalmente por los actividades delictivas establecidas de conformidad con esta Convención, cometidas en su beneficio por cualquier persona natural que actué ya sea individualmente o como parte de un órgano interno de la misma".

Por otra parte, la sección 2 del capítulo II contiene las condiciones y principios que han de orientar las normas de procedimiento en materia de delitos informáticos. En tal sentido, el artículo 15 de la Convención dispone que los Estados firmantes deberán velar por la adecuada protección de los derechos humanos a la hora de la adopción y aplicación de las normas de procedimiento penal relacionadas con los delitos informáticos.

Adicionalmente, en esta misma sección están contempladas algunas medidas judiciales concretas, a saber: (1) Medidas cautelares tendientes a la preservación de la integridad y custodia de datos informáticos; (2) Medidas tendientes a obtener la divulgación total o parcial de datos informáticos; y (3) Órdenes de búsqueda y allanamiento de datos informáticos almacenados en sistemas de cómputo; (4) Órdenes para la recolección e interceptación de datos informáticos en tiempo real. Estas medidas u órdenes, emitidas por autoridad competente, de conformidad con las disposiciones normativas internas que adopten los Estados signatarios, podrán ser dirigidas tanto a individuos como a proveedores de servicios de interconexión informática (ISP, Internet Service Providers) que estén domiciliados o establecidos, respectivamente, dentro del territorio nacional de cada Estado.

Finalmente, la sección 3 reconoce los distintos ámbitos de competencia en los que es viable ejercer la acción penal sobre aquellos delitos descritos en la sección 1. En este contexto, queda establecido, salvo reserva hecha por el Estado, que tendrán competencia las autoridades nacionales en cualquiera de las siguientes circunstancias: (1) Cuando el delito sea cometido dentro del territorio del Estado; (2) Cuando el delito sea cometido a bordo de un buque con la bandera del Estado;

(3) Cuando el delito sea cometido a borde de una aeronave con la bandera del Estado; y (4) Cuando el delito sea cometido por alguno de sus nacionales, si éste es punible de acuerdo con las leyes del lugar en que fue cometido, o si fue perpetrado fuera de la jurisdicción territorial del Estado.

La Convención sobre Delitos Informáticos constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. La misma tiene lugar en momentos en que el Internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimidad, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades. Hoy, a pocos días de su firma, como una muestra evidente de la aplicación efectiva de sus normas sobre cooperación internacional, la actividad conjunta de autoridades policiales en países como Inglaterra y España ha permitido desmantelar un número considerable de células criminales dedicadas a la producción y comercialización de pornografía infantil a través del Internet. Corresponde ahora a los países latinoamericanos la responsabilidad de reconocer la importancia de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad, una sociedad que ha llegado a ser denominada por algunos como "sociedad de la información[64]".

3. Situación jurídica de los delitos informáticos en Argentina.

En la Argentina, aún no existe legislación específica sobre los llamados ***delitos informáticos***. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto Nº 165/94 del 8 de febrero de 1994.

[64] http://www.alfa-redi.org/rdi-articulo.shtml?x=1582 No. 042 - Enero del 2002

En dicho Decreto se definen:
Obras de software: Las producciones que se ajusten a las siguientes definiciones:

1. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.
2. Los programas de computadoras, tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por la computadora.
3. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

Obras de base de datos: Se las incluye en la categoría de "obras literarias", y el término define a las producciones "constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos".

De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa, entendiendo como cosas aquellos objetos materiales susceptibles de tener algún valor la energía y las fuerzas naturales susceptibles de apropiación, asimismo la situación legal ante daños infligidos a la información es problemática.

El paso mas importante que en este sentido se ha dado en Argentina, es la presentación ante el parlamento de dos importantes proyectos de ley creados para controlar los delitos informáticos. Damos aquí un ligero esbozo de uno de ellos.

- **Proyecto de Ley Penal y de Protección de la Informática (Senador Eduardo Bauza).**

El Senador Eduardo Bauza, en su proyecto señala en el artículo 24 de su proyecto, que la alteración, daño o destrucción de datos en una computadora base da datos o sistema de redes, se realiza exclusivamente mediante el uso de virus u

otros programas destinados a tal modalidad delictiva, y aunque existen otros medios de comisión del delito, estos no fueron incorporados al tipo legal por el legislador.

En cuanto al tipo penal de violación de secretos y divulgación indebida se circunscribe al correo electrónico, dejando de lado la figura de la información obtenida de cualquier computadora o sistema de redes. Asimismo, el Senador Bauza, incluye la apología del delito y agrava la conducta en caso de ilícitos de atentados contra la seguridad de la nación.

En materia de los accesos no autorizados, el proyecto Bauza, en el artículo 20 prevé, para que se configure el tipo penal, que la conducta vulnere la confianza depositada en él por un tercero (ingreso indebido), o mediante maquinaciones maliciosas (dolo) que ingresare a un sistema o computadora utilizando una password ajeno.

En materia de Uso indebido, este Proyecto en su Artículo 21, incluye en el tipo legal a aquel que vulnerando la confianza depositada en él por un tercero (abuso de confianza), o bien por maquinaciones maliciosas (conducta dolosa), ingresare a un sistema o computadora utilizando una password ajena, con la finalidad de apoderarse, usar o conocer indebidamente la información contenida en un sistema informático ajeno (no incluye la revelación). En tanto en el artículo 38 pena a toda persona física o jurídica, de carácter privado, que manipule datos de un tercero con el fin de obtener su perfil, etc. y vulnere el honor y la intimidad personal o familiar del mismo.

En materia de Sabotaje y daños, este Proyecto, en el artículo 23, prevé prisión de uno a tres años para aquél que en forma maliciosa, destruya o inutilice una computadora o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena en caso de afectarse los datos contenidos en la

computadora o en el sistema de redes. Se resalta que el tipo legal propuesto requiere malicia en el actuar. El artículo 24 también incluye malicia (en el actuar) para alterar, dañar o destruir los datos contenidos en una computadora, base de datos, o sistemas de redes, con o si salida externa. El medio utilizado, según la propuesta, es mediante el uso de virus u otros programas destinados a tal modalidad delictiva.

En cuanto a la Interceptación ilegal/apoderamiento, este proyecto aplica penas de prisión.

En materia de Violación de secretos (Espionaje / divulgación), este Proyecto propone gradualismo en la aplicación de la pena, agravamiento por cargo e inhabilitación para funcionarios públicos. Además, impone multas por divulgación.

En lo relacionado con Estafa y defraudación, este Proyecto reprime con pena de prisión al responsable de una estafa mediante el uso de una computadora[65].

4. La situación jurídica de los delitos informáticos en España.

En España, donde sí existe una legislación clara sobre delitos informáticos, dio este importante paso legislativo, reformando el código penal en el año 1995, en cuya reforma, se adicionaron al código una serie de artículos que venían a contemplar o mas bien a tipificar claramente una serie de delitos informáticos, que a la luz del antiguo código, no hubiera sido posible castigarlos. Son estos artículos los que a continuación señalamos:

[65] www monografias.com/trabajos/legisdelinf/legisdelinf.shtml .

Artículo 197

1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero[66].

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

[66] Artículos del Código Penal Español referentes a Delitos Informáticos
(Ley-Orgánica 10/1995, de 23 de Noviembre/
BOE número 281, de 24 de Noviembre de 1.995)

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201

1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1. Escalamiento.
2. Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
3. Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
4. Uso de llaves falsas.
5. Inutilización de sistemas específicos de alarma o guarda.

Artículo 239

Se considerarán llaves falsas:

1. Las ganzúas u otros instrumentos análogos.
2. Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3. Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.
4. A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante
3. consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1. Valiéndose de mecanismos instalados para realizar la defraudación.
2. Alterando maliciosamente las indicaciones o aparatos contadores.
3. Empleando cualesquiera otros medios clandestinos.

Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 263

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

a) Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
b) Que se cause por cualquier medio infección o contagio de ganado.
c) Que se empleen sustancias venenosas o corrosivas.
d) Que afecten a bienes de dominio o uso público o comunal.
e) Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenadores se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos

que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

1. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
2. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses[67].

[67] www.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html

5. Legislación sobre delitos informáticos en Chile.

Chile ha sido otro de los países latinoamericanos que ha demostrado tener legisladores actualizados, al corriente del desarrollo de la tecnología y conscientes del impacto social y jurídico que ella causa.

La muestra de ello, es la promulgación de la ley de delitos informáticos, promulgada el 28 de mayo del 2003, la que a continuación transcribimos:

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado[68]."

[68] Ley de delitos informáticos promulgada en Santiago de Chile por la Parlamento nacional chileno, el 28 de mayo del año 2003. http://www.mcconnellinternational.com/services/country/Chile.pdf

6. Legislación sobre delitos informáticos en Costa Rica.

En este sentido, el 24 de octubre del 2001, Costa Rica dio un paso muy importante, al promulgar una ley que reformaba el código penal vigente del país en algunos artículos que no resultaban eficientes ante la aparición de la variante informática, artículos que a continuación enumeramos[69]:

Artículo único.-Adiciónense al Código Penal, Ley Nº 4573, del 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos dirán:

"Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"*Artículo 217 bis*.- Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis. - Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese,

[69] http://www.virusprot.com/Archivos/Ldcostarica.doc

borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

7. Legislación sobre delitos informáticos en Perú.

En la república del Perú, no existe aún una ley que regule de manera directa el asunto de los delitos informáticos, lo que sí existe es un proyecto de ley presentado al congreso por el congresista Jorge Muñiz, el 18 de agosto de 1999. En este proyecto lo que se propuso fue hacer una modificación a algunos artículos del código penal vigente. Tales artículos son los siguientes:

Artículo único.- Incorporase al Código Penal, promulgado por Decreto Legislativo N° 635, el Capítulo XI, Delitos Informáticos, los artículos 208a y 208b; con los siguientes textos:

Artículo 208 a.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de la libertad no mayor de dos años, o con prestación de servicios comunitario de cincuenta y dos a ciento cuatro jornadas.

Artículo 209 b.- El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la

misma, en la base, sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.

Otro proyecto importante que se encuentra ante el congreso, es la ley contra la pornografía infantil, la que regula la pornografía infantil en general, también de manera concienzuda trata el factor Internet como medio de producción y transmisión de la pornografía infantil.

Entre los artículos más importantes que se proponen adicionar el código penal de dicho país, están los siguientes:

ARTICULO 1°. - Adicionase los artículos 183-B y 183-C al Capítulo XI -Ofensas al Pudor Público- del Código Penal, con el siguiente texto:

"Artículo 183-B. - Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos, o pornográficos con el objeto y fin de video grabarlos, fotografiarlos o exhibirlos mediante medios impresos, electrónicos o de un sistema de datos a través de cómputo o de cualquier otro mecanismo de archivos de datos, con o sin el fin de obtener un lucro, se le impondrán la pena privativa de libertad no menor de cinco ni mayor de doce años y con trescientos sesenta y cinco días multa".

"Al que fije, grabe, imprima actos de exhibicionismo corporal, lascivos o pornográficos, en que participen uno o más menores de dieciocho años, se le impondrá la pena de cinco a doce años de pena privativa de la libertad y de trescientos sesenta y cinco días multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, produzca, reproduzca, ofrezca, venda, arriende, exponga, publicite, haga accesible, distribuya o trasmita a través de un sistema de computo o cualquier otro mecanismo de archivo de datos, el material a que se refiere el presente artículo".

"Artículo 183-C. - Para los efectos de estos artículos se entiende por pornografía infantil, toda representación de un menor de edad dedicado a actividades explícitas reales o simuladas de carácter sexual, realizada a través de escritos, objetos, medios audiovisuales, electrónicos, sistemas de cómputo o cualquier medio que pueda utilizarse para la comunicación y que tienda a excitar sexualmente a terceros, cuando esta representación no tenga valor artístico, literario, científico o pedagógico."

Esta ley fue introducida al congreso peruano por la congresista Enith Chuquival Saavedra, el nueve de mayo del 2002[70].

8. Legislación sobre delitos informáticos en Venezuela.

Es menester reconocer que en materia de delitos informáticos, Venezuela es el país latinoamericano que a nuestro juicio se encuentra legislativamente más desarrollado, por contar desde el seis de septiembre del 2001, con una de las leyes más completas sobre delitos informáticos en Latinoamérica[71].

Está estructurada en tres títulos y 33 artículos. El primer título habla sobre generalidades o disposiciones generales, tales como el objeto de la ley y algunas definiciones importantes como Hardware, software, información, virus, bombas lógicas, etc. Una cosa muy importante a señalar dentro de este primer título es lo que señala el artículo 3. El habla sobre el caso en que los delitos se haya cometido en otro país, pero que surtió efecto en Venezuela, caso en que la ley somete al delincuente a las leyes venezolanas, con la sola excepción de que el delincuente haya sido juzgado ya por el mismo delito en su país de origen, Es nuestra opinión, que dicho artículo fue muy inteligentemente incluido ene esta ley, pues uno de los problemas mas frecuentes con los delitos informáticos, se dan

[70] http://delitosinformaticos.com/legislacion/peru.shtml
[71] http://www.informatica-juridica.com/anexos/anexo379.asp

esta circunstancias, en la que ante un delito de este tipo, se da un conflicto de espacial de leyes.

El segundo título que habla ya directamente de los delitos informáticos, se subdivide a su vez en cuatro capítulos. Esta división del título segundo, equivale al mismo tiempo a una clasificación que los legisladores venezolanos hacen de los delitos informáticos, clasificación que merece todo nuestro elogio por cuanto se basa de acuerdo al bien jurídico afectado en cada caso de delito informático. En cada delito informático que se va tipificando en esta ley se van estableciendo las correspondientes sanciones, las que no exceden los diez años de cárcel ni multas mayores de mil unidades tributarias

El capítulo I, se trata de los delitos contra los sistemas que utilizan tecnologías de la información, según la ley en mención estos delitos son: acceso indebido con penas agravadas cuando se trata de sistemas protegidos, sabotaje o daño a sistemas, interesante saber que se establece para este último una sanción específica de acuerdo al grado de culpabilidad.

Dentro de este capítulo se tipifican también la posesión de equipos o prestación de servicios de sabotaje, el espionaje informático, el que se llega a castigar hasta con ocho años de cárcel y por último dentro de esta categoría de delitos se ubica la falsificación de delitos informáticos, en el que hábilmente se tipifica no como protector de la fe pública o de la legalidad de los documentos, sino que dichos documentos aparecen protegidos, pro en calidad de información en estado de almacenamiento.

En el segundo capítulo se regulan los delitos informáticos que atentan contra la propiedad, en el que no solo se contemplan los delitos tradicionales ejecutados por medios informáticos, tales como el hurto y el fraude, sino que se mencionan figuras que son exclusivas del fenómeno informático como la obtención indebida

de bienes y servicios, el manejo y apropiación fraudulenta de tarjetas inteligentes y la posesión de equipos para falsificaciones.

Algo importante para destacar de este capítulo, es a diferencia que en él se establece entre el hurto y el fraude informático, diferencia que ya los doctrinarios habían propuesto. En el hurto al igual que en el fraude hay uso de tecnología informática para acceder, interferir y manipular un sistema con el fin de sacar un provecho económico en perjuicio de un tercero, pero la diferencia radica que para el fraude informático se requiere introducir información falsa al sistema para que este obre con error.

La privacidad de las personas no es un bien que se empieza a vulnerar con la aparición de la tecnología de las computadoras, pero sí es más susceptible desde hace un par de décadas cuando la tecnología hizo aparecer aparatos de espionaje cada vez mas sofisticados y que ahora con la era de la computación y la nanotecnología, se encuentran en la cúspide del modernismo y la eficiencia, estas razones hacen aparecer en el tercer capítulo del título II de esta ley, los delitos contra la privacidad de las personas y de las comunicaciones.

El primer delito que resulta sancionado en este apartado es la violación de la privacidad de la información de carácter personal, luego aparece contemplada la violación de la privacidad de las comunicaciones. Este último resulta castigado con prisión de hasta seis años. El tercer y último delito contemplado en este capítulo es la revelación indebida de data o información de carácter personal, acto que se sanciona hasta un tercio por encima de la pena normal si de dicho acto resulta beneficio económico para el actor.

Fundamental resulta el capítulo cuarto de este título segundo. Fundamental para la protección dela indemnidad sexual de los menores de edad pues en primer término resulta castigado el hecho de distribuir material a través de cualquier

medio electrónico informático sin las medidas para que se restrinja el acceso a los niños, niñas o adolescentes.

Como segundo y último delito contemplado en este apartado está la exhibición pornográfica de niños o adolescentes, delito que al igual que la mayoría de los delitos, tienen como pena máxima ocho años de cárcel.

El último capítulo de este título II, son los delitos contra el orden económico en el que básicamente se trata de proteger la propiedad intelectual y al consumidor, porque a pesar de que en la ley se hable de apropiación dela propiedad intelectual, no estaríamos hablando de cosa diferente si usamos el término pirateo informático. La otra figura delictiva que se menciona en este capítulo es la oferta engañosa, mediante la cual se trata de proteger al consumidor de no ser engañado sobre la calidad de determinados productos, usando para ello recursos informáticos.

Como toda ley que conocemos en su penúltimo título (El título III), trata de las disposiciones comunes, empezando por tratar sobre las agravantes que pueden aumentar la pena a imponer. Entre las más importantes hay que mencionar las que señalan la adquisición de contraseñas ajenas, la comisión mediante abuso de posición, etc. Luego dicho apartado habla sobre penas accesorias como decomiso de los equipos empleados, inhabilitación especial, trabajo comunitario, indemnización civil, entre otras.

Finalmente en sus disposiciones finales no se dice nada relevante que tengamos que mencionar acá, excepto su fecha de publicación anteriormente citada[72].

[72] El 06 de septiembre del año 2001.

9. Los delitos informáticos en Japón.

En el país nipón existe la "Ley sobre acceso ilegal a una computadora", número 128 de 1999, vigente a partir del 3 de febrero del 2000, en la que se ordena lo siguiente:

"Husei access kinski hou (Prohibición de actos sobre acceso ilegal a una computadora)"

"Artículo 3. Ninguna persona ejecutará un acto sobre acceso ilegal a una computadora."

"2. El acto de acceso ilegal a una computadora mencionado en el párrafo anterior significa un acto que encuadra en cualquiera de los siguientes supuestos:"

"(1) El acto de lograr disponer de una función específica que está restringida por una función de control para el acceso, operando cualquier computadora en específico y logrando tal acceso, mediante la introducción vía línea de telecomunicación o con la clave de identificación de otra persona para aquella función (que excluye los actos ejecutados por el administrador o responsable *del* acceso, quien ha implementado la función para controlar el acceso respectivo, o efectuados con la aprobación del responsable del acceso o del operador autorizado para usar dicha clave de identificación)."

"(2) El acto de lograr disponer de una función específica que está restringida por una función de control para el acceso, operando cualquier computadora en específico y logrando tal acceso, mediante la introducción vía línea de telecomunicación de cualquier información (que excluye un código de identificación) o comando que pueda evadir las medidas de seguridad implementadas por la función para el control del acceso en ese uso en específico (que excluye los actos ejecutados por el administrador o responsable del acceso, quien ha implementado la función para controlar el acceso respectivo, o dirigidos

con la aprobación del responsable del acceso; lo mismo aplicará en el supuesto siguiente)."

"(3) El acto de lograr disponer de una función específica que está restringida por una función de control para el acceso, operando una computadora en específico cuyo uso está restringido por una función para el control de dicho acceso instalada en otra computadora, que está conectada vía línea de telecomunicación a aquella computadora, introduciendo en ella, vía telecomunicación cualquier información o comando que pueda evadir la medida de seguridad respectiva."

"Prohibición de actos para facilitar claves de acceso a computadoras."

"Artículo 4. Ninguna persona proveerá la clave de acceso de otra persona, relacionada a una función de control para el acceso a otra persona distinta al administrador de accesos designado para ese acceso o al usuario autorizado para esa clave de acceso, en el entendido de que se trata de la clave de acceso para ese acceso y computadora en específicos, o a solicitud de una persona que tiene dicha información, exceptuando el caso en el que los actos son efectuados por el administrador de accesos o con la aprobación del mismo o del usuario autorizado."

"Reglas penales."

"Artículo 8. La persona que sea responsable conforme a cualesquiera de los siguientes supuestos será castigada con servidumbre criminal (servicio comunitario) por un lapso no mayor a un año o al pago de una multa no mayor a 500,000 yenes:"

"(1) La persona que haya infringido la regla del Artículo 3, párrafo 1;"

"Artículo 9. La persona que haya infringido la regla del Artículo 4 será castigada con el pago de una multa no mayor a 300,000 yenes."

10. Los delitos informáticos en Los Estados Unidos de América.

En los Estados Unidos de América existe una legislación de carácter federal, denominada "Código de los Estados Unidos", en la que bajo el Título 18 "Delitos y Procedimiento Penal, Parte 1 de los Delitos, Capítulo 47 "Fraude y declaraciones falsas", reformada en el 3 de octubre de 1996, Sección 1030 de "Fraude y actividades relacionadas a las computadoras", se sanciona lo siguiente:

a) Quien sea que:

1. Teniendo conocimiento, acceda a una computadora sin autorización o excediendo la autorización a dicho acceso, y por medio de esa conducta haya obtenido información que haya sido determinada por el Gobierno de los Estados Unidos, mediante una orden del Ejecutivo o estatuto que ordene la protección en contra de divulgación prohibida por razones de defensa nacional o relaciones exteriores, o cualquier área restringida, como se señala en el párrafo "y" de la sección 11 del Acta de Energía Atómica de 1954, con la que se presuma que dicha información podría ser usada en perjuicio de los Estados Unidos, o en beneficio de cualquier nación extranjera, y que con plena intención comunique, entregue, transmita o provoque la comunicación, entrega o transmisión de tal información a cualquier persona que no tenga el derecho para recibirla, o con plena intención retenga la misma y no la devuelva a pesar de ser requerido al oficial o empleado de los Estados Unidos autorizado para recibirla."
2. Intencionalmente acceda a una computadora sin autorización o exceda dicha autorización y que por ello obtenga:

A) Información contenida en un registro financiero de una institución financiera, o de un tarjeta-habiente de acuerdo a lo establecido en la Sección 1602 (n) del Título 15, o contenida en un expediente de un consumidor en un Buroe de Crédito, de acuerdo a los términos definidos en el "Acta sobre Reportes permitidos de Crédito" (15 U.S.C. 1681 et seq.);"

B) Información de cualquier departamento o agencia de los Estados Unidos; o"

C) Información de cualquier computadora protegida si la conducta involucra una comunicación interestatal o comunicación no nacional;

3. Intencionalmente, sin autorización para acceder a una computadora no pública de una departamento o agencia de los Estados Unidos, acceda a dicha computadora del departamento o agencia, que sea de uso exclusivo del Gobierno de los Estados Unidos o, en el caso de una computadora no exclusiva para dicho uso, sea usada en nombre del Gobierno de los Estados Unidos y tal conducta afecte su uso por el Gobierno de los Estados Unidos."
4. Con conocimiento y con la intención de defraudar, acceda sin autorización a una computadora protegida, o exceda el acceso autorizado, y por medio de esa conducta se encamine al fraude en sí y obtenga cualquier ganancia, a menos que el objeto del fraude y la ganancia obtenida consista sólo para el uso de la computadora y el valor de dicho objeto no sea mayor a $5,000 (Dólares de los Estados Unidos de América) en el periodo de un año."
5. Con conocimiento provoque la transmisión de un programa, información, código o comando y como resultado de dicha conducta, intencionalmente cause daño sin autorización a una computadora protegida;"
    A. Intencionalmente acceda sin autorización a una computadora protegida y como resultado de tal conducta cause daño imprudentemente;"
    B. Intencionalmente acceda sin autorización a una computadora protegida y como resultado de tal conducta cause daño;"
6. Con conocimiento y con la intención de defraudar negocios (como se define en la Sección 1029) en cualquier clave de acceso o información similar relacionada a la que una computadora pueda ser accesada sin autorización, si:
    A. Dichas negociaciones afectan el comercio interestatal o comercio exterior; o
    B. Tal computadora es usada en nombre del Gobierno de los Estados Unidos.

7. Quien con la intención de extorsionar a cualquier persona, empresa, asociación, institución educativa, institución financiera, entidad gubernamental u otra entidad legal, cualquier dinero o artículo de valor, transmita en comercio interestatal o comercio extranjero cualquier comunicación que contenga cualquier clase de amenaza para causar daño a una computadora protegida, será castigado de acuerdo a la subsección (c) de esta sección.

a) Quien sea que intente en cometer un delito bajo la subsección (a) de esta sección será castigado como se señala en la subsección (c) de esta sección."
b) El castigo por un delito bajo la subsección (a) o (b) de esta sección consiste en:

1. Una multa bajo este título o prisión por un plazo no menor a 10 años, o ambas, en el caso de un delito bajo la subsección (a) (1) de esta sección que no sucede después de cumplir sentencia por otro delito bajo esta subsección, o una tentativa de cometer un delito sancionable bajo este subpárrafo; y
2. Una multa bajo este título o prisión por un plazo no mayor a 20 años, o ambos, en el aso de un delito bajo la subsección (a) (1) de esta sección que sucede después de haber compurgar prisión por otro delito bajo esta subsección, o una tentativa a cometer un delito sancionable bajo este subpárrafo; y"

2.1) Una multa bajo este título o prisión por un plazo no mayor a 1 año, o ambos, en el caso de un delito bajo la subsección (a) (2), (a) (3), (a) (5) (C) o (a) (6) de esta sección que no sucede después de haber compurgado pena por otro delito bajo esta subsección, o una tentativa a cometer un delito sancionable bajo este subpárrafo; y

2.2) Una multa bajo este título o prisión por un plazo no mayor a 5 años, o ambos, en el supuesto de un delito bajo la subsección (a) (2) si:"

i) El delito fuese cometido con propósito de ganancia comercial o financiamiento privado;"

ii) El delito fuese cometido fomentando cualquier acto criminal o tortuoso en violación de la Constitución o leyes de los Estados Unidos; o"

"(iii) El valor de la información obtenida excede de $5,000 (Dólares de los Estados Unidos de América);"

C) Una multa bajo este título o prisión por un plazo no mayor a 10 años, o ambas, en el caso de un delito bajo la subsección (a) (2), (a) (3) o (a) (6) de esta sección que ocurre después de compurgar pena por otro delito bajo esta subsección, o una tentativa para cometer un delito sancionable bajo este subpárrafo; y"

2.3) Una multa bajo este título o prisión por un plazo no mayor a 10 años, o ambos, en el caso de un delito bajo la subsección (a) (4), (a) (5) (A), (a) (5) (B), o (a) (7) de esta sección que no sucede después de compurgar pena por otro delito bajo esta sección, o una tentativa para cometer un delito sancionable bajo este subpárrafo; y

2.3.1 Una multa bajo este título o prisión por un plazo no mayor a 10 años, o ambos, en el caso de un delito bajo la subsección (a) (4), (a) (5) (A), (a) (5) (B), o (a) (5) (C) , o (a) (7) de esta sección que sucede después de compurgar pena por otro delito bajo esta sección, o una tentativa para cometer un delito sancionable bajo este subpárrafo; y"

2.3.2 El Servicio Secreto de los Estados Unidos será, en adición a otra agencia con autoridad, quien tenga la autoridad para investigar delitos bajo las subsecciones (a) (2) (A), (a) (2) (B), (a) (3) y (a) (4), (a) (5) y (a) (6) de esta sección. Tal autoridad del Servicio Secreto de los Estados Unidos será ejercida en atención al convenio que deberá celebrarse entre el Secretario del Tesoro y el Procurador General."

2.3.3 Esta sección no prohibe cualquier investigación legal con autorización, protectora, o actividad de inteligencia o de cualquier agencia con autoridad legal de los Estados Unidos, o Estatal, o subdivisión política de un Estado o de una agencia de inteligencia de los Estados Unidos."

2.3.4 Cualquier persona que sufra daño o perjuicio por una violación a esta sección podrá ejercer una acción civil en contra del perpetrador, para obtener daños compensatorios, resarcimiento moral o cualquier otro resarcimiento. Daños por violaciones sobre daño como está definido en la subsección (e) (8) (A) están limitados a daños económicos. Ninguna acción será ejercida bajo esta subsección a menos que dicha acción sea instaurada dentro del plazo de 2 años contados de la fecha del acto motivo de la acción, o a partir de la fecha en que se tenga conocimiento del daño."

2.3.5 El Procurador General y el Secretario del Tesoro deberán reportar anualmente al Congreso, durante los primeros 3 años siguientes a la promulgación y vigencia de esta subsección, sobre investigaciones y juicios bajo la sección 1030 (a) (5) del Título 18, del Código de los Estados Unidos[73].

11. Los delitos informáticos en el contexto legal nicaragüense.

Hay una clara diferencia entre nuestra realidad jurídica y la de los países que hemos señalado en este capítulo. NO obstante, vamos a detenernos un poco en cada una de las leyes que de alguna manera u otra se relacionan al tema, a fin de ir señalando el grado de perspicacia de nuestros legisladores para darse cuenta del desarrollo de la tecnología y de las implicaciones jurídicas que ello siempre trae consigo.

Para empezar, vamos a hacerlo con la ley más importante del ordenamiento jurídico de cada país. La constitución política.

[73] http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

12.1. La constitución política y los delitos informáticos.

Siendo Nicaragua un Estado de Derecho, en el que la constitución está en la cúspide del ordenamiento jurídico y tomando en cuenta el principio de la supremacía de la constitución, ninguna ley o norma jurídica de rango inferior puede contradecir lo contemplado en ella, el legislar sobre delitos informáticos no representa problema constitucional alguno, dado que la constitución en sus artículos 25 y 26 Cn determina la existencia de algunos derechos individuales fundamentales que pueden resultar vulnerados con la comisión de los delitos informáticos; entre los cuales están el derecho a la privacidad, la seguridad y el respeto a la honra y la reputación de las personas[74].

12.2. Los delitos informáticos y el código penal.

Está claro que nuestro código penal no ha tenido modificación importante en materia de delito informáticos que tengamos que mencionar aquí, pero en todo caso la mayoría de los delitos informáticos son delitos tradicionales ejecutados por medios no tradicionales[75], pero que no se pueden resolver con las normas de nuestro código en mención por no tener contemplada específicamente tales circunstancias y por ser prohibida en materia penal la interpretación extensiva.

Pese a lo anterior es en el código penal en donde se encuentran muchas de las figuras antecesoras de las que en el desarrollo de nuestra monografía hemos llamado delitos informáticos y que con la modificación y adición correspondiente serían capaces de regular todas estas situaciones que en la presente investigación hemos venido describiendo. Tales figuras son por ejemplo:

- La corrupción de menores[76](Arto 201)

[74] Constitución política de Nicaragua / décimo tercera edición, Editorial Jurídica, año 2006. Pág. 10.
[75] Tal como lo son los medios informáticos.
[76] Figura dentro de la cual cabe la Prostitucion infantil

- Los delitos contra la confidencialidad, como es la violación y divulgación de correspondencia (arto 238 y sgtes). Ambas son acciones que muy frecuentemente se dan en el Internet, en el que personas mal intencionada con las herramientas y las conocimientos necesarios pueden interceptar y conocer el contenido de los correos electrónicos y de muchas otras formas de comunicación que se dan en la red.
- Los delitos contra la propiedad. Especialmente el robo, el hurto y la estafa, tienen su modalidad informática y que para ser regulados por nuestra legislación penal, urge una reforma en este sentido[77].
- Los daños. También incluidos dentro del ámbito de los delitos contra la propiedad, pero que por sus múltiples modalidades se reviste de mucha importancia, porque aunque en el código no tenga más de tres artículos[78], en los delitos informáticos se efectúa de diversas modalidades como la destrucción de hardware y el sabotaje en sus diversas modalidades(Virus, bombas lógicas, gusanos, etc)
- Delitos contra la fe pública. Todos ellos contenidos dentro del título IX del libro II de nuestro código penal. En los seis capítulos de este título se abarcan las modalidades conocidas de falsificación tales como la falsificación de moneda, de documentos públicos y privados, etc. Lo que tenemos que recalcar en cuanto a esto es que con la correcta interpretación de las normas aludidas, es posible castigar conductas delictivas a las que se les adjudica el adjetivo de informáticas, pues en el caso de las falsificaciones no lo son por el fin, sino por el medio. Esto es porque hay muchas falsificaciones de monedas, de documentos públicos, de instrumentos privados, etc los que se utiliza la computadora y toda la tecnología anexa para pero que la conducta encaja muy bien en los tipos penales establecidos.
- Finalmente, creemos que en una futura reforma de nuestro código penal a fin de hacerlo capaz de regular los delitos informáticos, también se harían

[77] Artos 263, 266, y 283 pn.
[78] Artos 293, 294 y 295 Pn.

adiciones a los artículos que hablan de la asociación para ilícita para delinquir y el terrorismo[79]. Afirmamos tal caso en vista de que actualmente existen sitios en Internet en donde abiertamente se promuevan actos que constituyen delitos como la prostitución infantil y mas aún, existen grupos de terrorismo muy conocido con sitios oficial en Internet en donde promueven sus ideas y tratan de ganar adeptos[80].

12.3 La ley de derechos de autor.

Entre todos los delitos informáticos que hemos mencionados en la presente monografía, los que atacan los derechos del autor son los que con mayor frecuencia y facilidad podemos observar en nuestro entorno. Muchísimas empresas, personas jurídicas y naturales, tienen sistemas informáticos que en su mayoría funcionan a base programas (software) piratas[81]. Y no es el único ejemplo, la música que el noventa y cinco por ciento de la población compra, es pirateada. Bien sea a partir de un disco original, usando computadoras o la tecnología necesaria, o bien puede ser pirateada a través de Internet y luego quemada en CDs que luego nosotros compramos. Por todas estas razones es que necesitamos detenernos a observar lo que al respecto la ley sobre derechos de autor que tenemos en nuestro país.

Claro está que a la luz de la citada ley, tales conductas están prohibidas y sancionadas, porque no se tratan de nuevos delitos ya que como muchos otros lo son por el medio utilizado y no por el fin, pero el problema de ellos radica en la capacidad de las instituciones responsables para hacer cumplir la ley a tantos infractores. De todas formas en dicha ley, es en el artículo 106 donde se contemplan las violaciones y las sanciones penales a imponerse. Detengámonos en el inciso 5 de dicho artículo, en donde se castiga con prisión de uno a dos años el que retransmita por cualquier medio alámbrico o inalámbrico una emisión de

[79] Artos 493 y 499 Pn.
[80] Código penal de Nicaragua / Sergio Cuaresma Terán – 2da ed.—Managua: HISPAMER, 2001
[81] Los entendidos en la materia afirman que en Nicaragua, mas del 80% de las computadoras funcionan a base de programas piratas.

radiodifusión o televisión, sin la autorización del titular de la emisión. Igual atención pongamos al inciso 1, del artículo 107, en donde se castiga hasta con tres años al que sin autorización por escrito del particular, reproduzca u obtenga copias de obras o fonogramas por cualquier medio o procedimiento en forma original o modificada, íntegra o parcialmente. En conclusión a este apartado, podemos afirmar que en este tipo de delitos informáticos que atacan la propiedad intelectual, se trata únicamente de una correcta interpretación y aplicación de la norma correspondiente para castigar las conductas mencionadas[82].

12.5. El proyecto de ley del nuevo código penal.

El 26 de noviembre del año 2003, la comisión de justicia de la Asamblea Nacional, presidida por el Diputado Dr. Orlando Tardencilla, dirigió una carta al Dr. Jaime Cuadra Somarriba entonces Presidente de la Asamblea Nacional. En dicha carta la comisión en cuestión emitía un dictamen favorable (a excepción de algunas sugerencias) al proyecto de ley de un nuevo código penal para el país. Destacamos que ese ha sido el paso mas importante que ha tenido, es haber sido aprobado en lo general durante la legislatura pasada, pero dista mucho para que finalmente sea aprobado en lo particular y así se pueda promulgar, dado que desde hace mucho tiempo el parlamento no ha podido darle la prioridad necesaria para ubicarlo en la agenda legislativa.

En general, es un código moderno e innovador, entro otras razones por las siguientes:

- ☆ La relativamente novedosa clasificación tripartita de las infracciones.
- ☆ Las modificaciones habidas en cuanto al sistema de penas, medidas de seguridad y responsabilidad civil.

[82]Ley de derechos de autor y derechos conexos, "La Gaceta, diario oficial" No 167, Ley # 312, 1ro de septiembre de 1999.

- ☆ La nueva cláusula para *las actuaciones en nombre de* otros y para extender la autoría en delitos especiales en donde ciertas exigencias de tipo recaen hasta en personas jurídicas[83].

Vemos pues que entre las principales innovaciones del Anteproyecto en cuestión no encontramos referencia directa a delitos informáticos, no está completo en este sentido. Sin embargo, sí hay algunos artículos en el anteproyecto que merecen nuestra atención, en cuanto prevén circunstancias muy actuales, prevén el desarrollo dela informática o la telemática, como una potencial y efectiva herramienta en la comisión de algunos delitos.

El artículo 191 del proyecto en mención, castiga hasta con dos años de prisión al que al margen de la ley abra, intercepte o por cualquier medio un pliego cerrado o un despacho telegráfico, telefónico, telemático, electrónico o de otra naturaleza que no le esté dirigido. Observemos que en el artículo citado se estaría castigando aún sin mencionarlo la intercepción de e-mail, delito informático bastante frecuente en la vida virtual.

De esta forma es posible encontrar otros artículos que una vez aprobado el proyecto de ley estarían regulando muchas de las actividades que hemos catalogado aquí como delitos informáticos. El artículo 196 (Por ejemplo), prohíbe la comercialización de banco de datos, el 197 castiga la utilización no autorizada y el ingreso no autorizado a registros informáticos o banco de datos; esto sería lo que en esta monografía hemos llamado accesos no autorizados.

Otro delito informático que claramente regula este nuevo código, es la estafa informática contenida en el arto. 227, contenida en el título “Los delitos contra el patrimonio y el orden socio-económico”, aparece como una modalidad de la estafa tradicional, claro estableciendo la diferencia que en esta última se induce al error a

[83] José Luis Gonzáles Cussac. Catedrático de derecho penal de la Universidad Jaime I. (España)

una persona, pero en la primera (la estafa informática) lo que se requiere es una manipulación de registro o programa informático.

Un delito que podremos llamar meramente informático, es el que establece el 243, que habla dela destrucción de registros informáticos. Es muy importante resaltar de este artículo, que en su texto se está claramente señalando como objeto de protección la información almacenada en sistemas informáticos, lo que significa que una vez promulgado este nuevo código penal, podremos hablar de la información como nuevo bien jurídico protegido en la tipificación de los delitos informáticos. No menos interesante resulta el artículo 244 que habla del uso de programas destructivos. Aunque el texto no lo mencione directamente, pero este artículo sería de aplicación inmediata ante el caso de virus, bombas lógicas o gusanos, las tres modalidades del sabotaje informático.

Luego, los delitos informáticos contra la fe pública y la seguridad del Estado, son los que al igual que con el actual código podrían con una adecuada exégesis podrían subsumirse en los artículos correspondientes. En general, a como lo habíamos dicho el anteproyecto es moderno e innovador en cuanto al tema que aquí nos ocupa, pues contiene tipos que no tiene el actual y que una vez aprobado, Nicaragua habría dado un paso muy significativo en la regulación de este fenómeno internacional que es propiciado por el desarrollo actual dela tecnología informático, sin embargo existen muchos delitos informáticos que quedan fuera del contenido de este anteproyecto de ley, por lo que aun cuando dicho proyecto esté aprobado, va a ser necesario la emisión de una ley especial como lo hizo Venezuela, para regular de manera completa y efectiva los delitos informáticos, a menos de que nuestros legisladores prefieran modificar el proyecto de ley e incluir en el de una vez todas estas figuras que conocemos como delitos informáticos y así tener un cuerpo de normas penales mas extenso, completo, moderno y efectivo.

CONCLUSIONES.

El desarrollo de las ciencias y la tecnología, especialmente la tecnología informática, ha sido de tal magnitud que ha planteado para el Derecho la regulación de novedosas situaciones, razón por la cuál surge el Derecho informático, el que está integrado por las disposiciones legales que regulan el tratamiento de la información. No obstante las diferentes posiciones doctrinales sobre la naturaleza de este nuevo Derecho, predomina la que sostiene que el Derecho informático es un Derecho autónomo por tener la existencia de un campo normativo, docente, institucional y científico.

Precisamente una de las novedades que ha traído consigo el desarrollo de las tecnología informática ha sido la aparición de una gama nueva de actos que por el dolo que los caracteriza y los perjuicios que causan, se han denominados Delitos informáticos. La mayoría de ellos son figuras delictivas tradicionales ejecutadas a través de formas no tradicionales, sin embargo otros son totalmente novedosos como la destrucción de base de datos, la creación de virus informáticos y los accesos no autorizados, etc.

Para hablar con propiedad sobre los Delitos informáticos, es necesario primero diferenciarlos claramente de los delitos electrónicos, dado que ambos términos no resultan sinónimos, ya que en los electrónicos básicamente se protege la integridad física de un bien electrónico, en cambio en los delitos informáticos el número de bienes jurídicos que podrían salir perjudicados es amplio. Otra cuestión muy importante a plantearse en este tema, es si en los Delitos informáticos existe un nuevo bien jurídico protegido o si por el contrario solo se protegen los bienes jurídicos tradicionales afectados por delitos ejecutados con instrumentos modernos y formas no tradicionales. Sobre esta pregunta nos hemos inclinado por la postura de la Dra. Sandra Jeannette Castro, que afirma que en el caso de algunos delitos informáticos sí existe un nuevo bien jurídico llamado “información”,

bien que resulta afectado en el caso de la destrucción de base de datos o en el caso del daño lógico a través de virus informáticos.

No solo hemos hablado de la existencia de un nuevo bien jurídico sino que también lo hemos clasificado de intermedio, por cuanto la información posee todas las características de los bienes jurídicos intermedios como Suprapersonalidad, estar vinculado a un bien jurídico netamente personal, pertenecer al ámbito de los intereses de la comunidad y no del Estado, entre otros.

Una característica muy importante de los delitos informáticos es su similitud con los delitos de cuello blanco, pues la posibilidad de cometerlos es reducida a cierto grupo de personas, sin embargo es muy difícil determinar la cantidad exacta de pérdidas económicas que en muchos países dejan cada año, dado las facilidades de clandestinidad que caracterizan estos delitos y por otro lado en muchos casos, por la falta de recursos y preparación técnica de las autoridades correspondientes.

Es muy importante señalar que la mayoría de los países europeos han tenido importantes progresos legislativos al crear leyes especiales contra delitos informáticos, o bien modificando adecuadamente sus códigos penales, tal como lo hizo España en el año 1995. Incluso muchos países latinoamericanos ya tienen legislación importante sobre la materia, países como Chile, Venezuela y Costa Rica. Nicaragua aún no tiene algún tipo de norma que regulen los delitos informáticos, aparte de las normas aplicables a la piratería o los artículos del código penal vigente que con la correcta hermenéutica resulten aplicables a situaciones delictivas en el que la informática fue parte importante. El mas importante paso que en este sentido esté en algunos artículos dispersos en el proyecto del nuevo código penal, en el que se castigan conductas que podrían catalogarse como delitos meramente informáticos, aunque por otra parte no se vislumbre aún la posibilidad latente de una pronta aprobación de dicho proyecto.

Es importante que en Nicaragua se legisle sobre delitos informáticos, no solo para modernizar su Derecho y encausarse mejor en el proceso de globalización, sino también para hacer mas efectiva la lucha internacional contra este tipo de delitos.

RECOMENDACIONES.

Es muy importante que Nicaragua tenga cuerpos normativos modernos, para encarar con mayor eficacia el desafío que plantea el actual proceso de globalización y el desarrollo de las nuevas tecnologías. Es por ello que consideramos importante que se cree una Ley que venga a regular directamente los delitos informáticos, sin olvidar el carácter extraterritorial que ellos tienen. Debe ser una ley que permita no solo declarar culpable al que cometió un acto que ella misma determine como delito informático, sino que haga el proceso posible aún cuando el acto se haya cometido en jurisdicción internacional pero que sus consecuencias se sufran en Nicaragua, de igual forma cuando el ilícito se dio en Nicaragua pero con consecuencias extraterritoriales, situación en la cual no es bueno para Nicaragua que su falta de legislación en la materia sea obstáculo para el justo castigo de tales conductas.

En realidad no se debe legislar únicamente sobre delitos informáticos, porque no sería una completa modernización del Derecho positivo nicaragüense sin regular los otros campos del Derecho informático, tales como protección de datos, protección jurídica del software, contratación electrónica, firma digital, etc. Para tal fin sería ideal la creación en nuestra Asamblea Nacional, de una comisión que vele por la actualización de todo los cuerpos normativos, para que estos se correspondan con las circunstancias de los nuevos tiempos y así en materia de Derecho informático sepa determinar el momento en que se hace necesario crear las normas que en otros países conforman un verdadero Derecho positivo informático.

Por otro lado, las universidades que ofrecen la carrera de Derecho deberían al menos durante un semestre ofrecer la cátedra de Derecho informático como parte del afán de formar profesionales modernos de educación sólida y de alta calidad. Creemos que nuestra facultad podría empezar a dar los primeros pasos en este

sentido al organizar seminarios sobre Derecho informático, al invitar a los más entendidos en la materia a brindar conferencias en nuestros auditorios para nuestros estudiantes, y así actividades similares.

BIBLIOGRAFIA

1. Barreda Gonzáles, Nadiezhda Krúpskaya y otros / Derecho informático: contenido y aplicación. – León, Nic.: UNAN; 2002.

2. Davara Rodríguez Miguel Ángel, Manual de Derecho informático, Edición 1ª, --Pamplona Arazandi, 1997.

3. Diccionario Nuevo mundo Lengua Española – Ediciones Nuevo Mundo – Dirección Gustavo A. Dos Santos – España 1999

4. Castellón Barreto Ernesto y Hernández León Luis / Apuntes de Derecho penal.- - Nic.:Editorial universitaria, 1998.

5. Constitución política de la República de Nicaragua / 13ª Edición.—Editorial jurídica.: Managua, 2006.

6. Chacón Pantoja Rina María y Gámez Valle Ligia María / Los delitos informáticos como bien jurídico protegido en materia penal.- - León, Nic.: UNAN-León, 2003.

7. Cuaresma Terán, Sergio / Código penal de Nicaragua.- - 2ª Ed.-- Managua: Hispamer, 2001.

8. Ley de derechos de autor y derechos conexos, “La gaceta Diario oficial” No. 166, ley # 312, 31 de Agosto de 1999.

9. Ley de derechos de autor y derechos conexos, “La gaceta Diario oficial” No. 167, ley # 312, 1º de septiembre de 1999.

10. Luzón Peña, Diego Manuel / Curso de Derecho penal: Parte general.- -1ª Ed, Managua, Nic.:. Hispamer 1999.

11. Mata y Martín, Ricardo M. / Delincuencia informática y Derecho penal.- -1ª Ed, Managua, Nic.: Hispamer, 2003.

12. Monjarrez Salgado, Luis / Introducción al estudio del derecho, Tomo I.- - León, Nic.: UNAN-León, Bitecsa 2002.

13. Navas Mendoza, Azucena / Curso básico de Derecho mercantil, Tomo I. – León, Nic.: Editorial universitaria UNAN-León, 2003.

14. Pérez Luño Antonio Enrique / Manual de informática y Derecho.- - Editorial Ariel.: Barcelona 1996.

15. Proyecto de ley del nuevo código penal de la República de Nicaragua.

16. Téllez Valdés, Julio / Derecho informático.- -2ª Ed. McGraw-Hill.: Mexico, 1996.

17. Valladares Castillo Francisco / Manual de Derecho individual del trabajo y seguridad social. – León, Nic.: Bitecsa, 2001.

Páginas Web consultadas.

- http://comunidad.derecho.org/gmontoya
- http://comunidad.derecho.org/gmontoya/files/info04.htm
- http://delitosinformaticos.com/legislacion/peru.shtml
- http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node77.html
- http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico
- http://es.wikipedia.org/wiki/Derecho_laboral
- http://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico
- http://yaleglobal.yale.edu/display.article?id=4029
- http://www.alfa-redi.org/rdi-articulo.shtml?x=212
- http://www.alfa-redi.org/rdi-articulo.shtml?x=398
- http://www.alfa-redi.org/rdi-articulo.shtml?x=1480
- http://www.alfa-redi.org/rdi-articulo.shtml?x=1582
- http://www.angelfire.com/freak2/dubi/DI.htm
- http://www.cinu.org.mx/11congreso/UN/prensa.htm
- http://www.delitosinformaticos.com/delitos/colombia1.shtml
- http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.31.htm
- http://www.elrinconcito.com/articulos/DelitosInf/legisdelinf.htm
- http://www.informatica-juridica.com/anexos/anexo379.asp
- http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo10.htm
- http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo14.htm
- http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo35.htm
- http://www.maximail.com/delitosinformáticos/espionaje
- http://www.mcafee.com/es/antipiracy_policy.htm
- http://www.mcconnellinternational.com/services/country/Chile.pdf

- http://www.monografias.com/trabajos23/juridica-informatica/juridica-informatica.shtml
- http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
- http://www.portaley.com/delitos-informaticos/espionaje.shtml
- http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm
- http://www.uoc.edu/in3/dt/20056/
- http://www.virusprot.com/Archivos/Ldcostarica.doc
- www.desolapate.com/Conferencia%20Delitos%20Informaticos.htm
- www.jura.uni-muenchen.de/einrichtungen/ls/sieber/prof.htm
- www.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html
- www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo11.htm
- www.mailxmail.com/curso/informatica/**delitos**informaticos/capitulo22.htm
- www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo39.htm
- www.monografîas.com/trabajos/legisdelinf/legisdelinf.shtm
- www.proasetel.com/paginas/articulos/**sabotaje**_informatico.htm
- www.solocursos.net/pornografia_**infantil**_e_internet-slccurso1110235.htm
- www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap5.htm

ANEXOS

ANEXO 1.

Ley especial contra los delitos informáticos de la República de Venezuela.

LA ASAMBLEA NACIONAL

DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

DECRETA

la siguiente,

Ley Especial Contra los Delitos Informáticos

Título I

Disposiciones Generales

Artículo 1

Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.-

Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3.

Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4.

-Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley

Artículo 5

Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente

Título II

De los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6.-

Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias

Artículo 7.-

Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.-

Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.-

Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Artículo 10.-

Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.-

Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.-

Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13.-

Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.-

Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.-

Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice

indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.-

Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.-

Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18-

Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.-

Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o

instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III

De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.-

Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.-

Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22.-

Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV

De los delitos contra niños, niñas o adolescentes

Artículo 23.-

Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o

reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.-

Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V

De los delitos contra el orden económico

Artículo 25.-

Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.-

Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III

Disposiciones comunes

Artículo 27.-

Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28.-

Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29.-

Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1º El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2º El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.
4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30.- Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31.- Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV

Disposiciones Finales

Artículo 32.-

Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela

Artículo 33. -

Derogatoria. Se deroga cualquier disposición que colida con la presente Ley.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.

William Lara
Presidente

Gerardo Saer Pérez
Segundo Vicepresidente.

Leopoldo Puchi
Primer Vicepresidente

Eustaquio Contreras.
Secretario.

Vladimir Villegas.
Subsecretario.

ANEXO 2.

Narcotráfico aprovecha internet.

Internet: la ausencia de legislación impide perseguir el tráfico de drogas.

Una organización de Naciones Unidas advirtió que la utilización de la red internet por los narcotraficantes está dificultando la lucha contra el uso de drogas ilícitas.

La Junta Internacional de Fiscalización de Estupefacientes (JIFE) señaló en su informe referente al año 2001 que drogas ilegales están siendo comercializadas a través de Internet, con la ayuda de la legislación que prohíbe monitorear comunicaciones en la red.

Los vendedores de drogas en Internet logran evadir la cárcel debido a que gran parte de los países no cuentan con legislación para los crímenes cibernéticos, señala el informe.

La JIFE, con sede en Viena, también destacó el liderazgo que tiene actualmente Birmania en la producción y venta de opio, luego de que el ex régimen Talibán destruyera las plantaciones de esta planta en Afganistán.

La junta también realizó un llamado para que los países detuvieran cualquier legislación destinada a la legalización de marihuana, señalando que sería "un error histórico" tratar la droga al mismo nivel que el alcohol y el tabaco.

Heroína: aumento del consumo en el mundo.

Crimen online

Un informe de la República Checa reveló que la droga estaba siendo distribuida con la ayuda de los cafés internet y los teléfonos celulares.

El informe también destaca que empresas holandesas estarían utilizando la red para vender semillas de marihuana y otros productos a diferentes partes del mundo.

También se descubrió el uso de cuentas de internet por parte de los traficantes para lavar dinero de la droga, y que farmacias estaban vendiendo drogas sin necesidad de prescripciones.

Birmania sustituyó a Afganistán como principal productor de opio.

"La JIFE está particularmente preocupada por aquellos países donde la ausencia de una legislación adecuada termine transformándolos en santuarios para los traficantes".

La junta también declara su preocupación por el incremento en el uso de droga intravenosa en África, lo que podría complicar aún más la situación del SIDA en la región.

En los últimos tres años, el uso de droga intravenosa en Sudáfrica se habría incrementado en un 40%.

En Estados Unidos, el uso de cocaína se mantiene estable, mientras que se muestra un incremento en el uso de heroína entre los jóvenes[1].

[1] http://news.bbc.co.uk/hi/spanish/science/newsid_1844000/1844137.stm

ANEXO 3.

Revelan cuantioso fraude informático

(18.05.2001): Debido a una vulnerabilidad en un software de carro de compras llamado "PDG" que expuso toda la información de los clientes de 4,000 sitios web, se han reportado muchos casos de fraude en los clientes de un sitio web llamado SawyerDesign.com.

A pesar que la falla fue detectada en abril y que el FBI emitió una alerta pública dirigida a los clientes del software, Regal Plastic Supply, los operadores de SawyerDesign.com, no se enteraron de la situación por lo que no aplicaron el parche que PDG Software emitió para reparar la vulnerabilidad.

En los días siguientes y hasta el fin de semana pasado, hackers hicieron cargos por miles de dólares en las tarjetas de crédito de las víctimas en sitios de apuestas, comprando tarjetas telefónicas y descargando software costoso.

"Tuve una horrorosa situación el mes pasado, tuve cargos por $6,000. Este mes por $2,000. La mayoría en sitios de apuestas y lugares como Firecash.com", dijo Hunter Culberson, una de las víctimas.

De acuerdo a la información, Regal Plastic nunca recibió el e-mail porque compró el software de un revendedor.

"Pensamos que habíamos comprado el mejor software del merado. No teníamos idea de que la solución de carro de compras estaba accesible para todos", señaló SawyerDesign.

Por su parte, el presidente de PDG, David Snyder, señaló antes de esto nunca habíamos tenido contacto con SawyerDesign". "Lo mejor que podemos hacer es publicarlo, le dijimos a los revendedores que necesitaban contactar a sus clientes directamente".

Aunque las víctimas no serán responsables de los cargos y ya se están eliminando los cobros de sus tarjetas de crédito, es muy probable que les quede el recuerdo de una mala experiencia[♣].

Anexo 4.

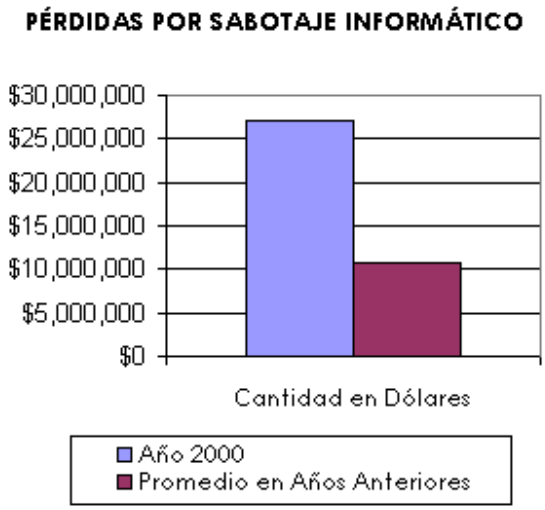
♣ www.diarioti.com/noticias/2001/may2001/15195124.htm

Estadísticas Sobre Delitos Informáticos.

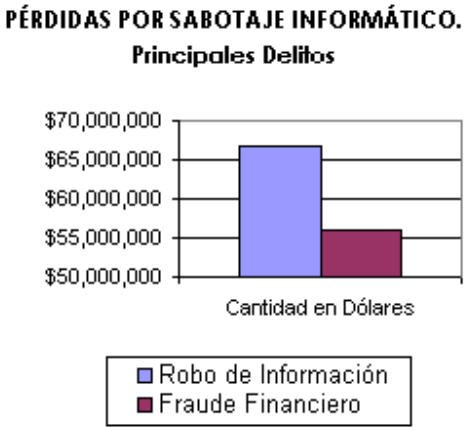
Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.
Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado «Estudio de Seguridad y Delitos Informáticos» realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.
Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.
Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:
Violaciones a la seguridad informática.
- No reportaron Violaciones de Seguridad 10%
- Reportaron Violaciones de Seguridad 90%

90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.
70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados - por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

Pérdidas Financieras.
74% reconocieron pérdidas financieras debido a las violaciones de las computadoras. -
Las pérdidas financieras ascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850. Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000). Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores[•].

[•] http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo18.htm

ANEXO 5.

Nicaragua Desarrolla Sociedad de la Información

De acuerdo al doctor Boyan Radoykov, especialista del programa de división de la sociedad de la información de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Nicaragua presenta una contraparte seria para el desarrollo de proyectos que desarrollen la sociedad de la información. Radoykov visitó Nicaragua invitado por la Secretaría de la Juventud (Sejuve), para conocer sobre el desarrollo de programas que involucran a los jóvenes, que apoyan la lucha contra el VIH/sida y desarrollan la sociedad de la información.

"Tuve la oportunidad de ver muchas iniciativas, discutir con mucha gente, tener una buena opinión de la situación actual y del potencial que existe. No se puede realizar cosas sin contraparte seria, gente con quien contar. Las ideas solas no valen nada si no hay gente para realizarlas", expresó Radoykov.

Agregó que en Nicaragua la contraparte seria está en la gente que tiene la experiencia, que conoce el asunto de la juventud, personas que no solamente saben de programas, políticas e iniciativas, sino que tienen la capacidad de desarrollar proyectos concretos. Radoykov señaló que la visita le dejó una visión clara de cómo la UNESCO puede trabajar con Nicaragua, de lo que se puede hacer, como y con quién.

Manifestó que el trabajo de la UNESCO con Nicaragua puede ir en varias direcciones. La primera sería amplificar el proyecto de prevención del sida y asegurar la sostenibilidad a medio plazo de este proyecto.

Señaló que se debe ver las posibilidades de extender el proyecto a otros países de la región, como El Salvador, Guatemala y Costa Rica, analizando las contrapartes que se encuentre en esos países.

"Los otros aspectos tocan a la promoción juvenil en el campo del empleo, autoempleo. Tenemos algunas ideas para apoyar el servicio voluntario con contactos, experiencias y nuevas ideas. Todo eso son oportunidades para fortalecer lo que se hace ya", añadió Radoykov.

APOYO A DISTINTAS ÁREAS

En relación al apoyo que la UNESCO brinda para desarrollar la sociedad de la información a nivel mundial, el especialista señaló que esa es su vida, lo que hacen cada día.

"Tenemos bastantes proyectos en todos los campos que toca. Educación a distancia, capacitación, formación de jóvenes y personas desfavorecidas en tecnologías de la información, trabajo con instituciones para el desarrollo de sofware, libros, y muchas otras cosas", explicó Radoykov. Añadió que sobre todo se está preparando la segunda cumbre de la sociedad de la información, que va a tener lugar en Túnez. La primera fue organizada el año pasado en Ginebra. "Son oportunidades para

destacar la importancia de la sociedad de la información como una herramienta para llegar a una sociedad del conocimiento", dijo.

EL MARCO JURÍDICO

Según el especialista, Nicaragua va encaminada al desarrollo de la sociedad de la información, con la creación de instituciones, comisiones que trabajan en ese campo, y leyes informáticas.

Nicaragua a través del Consejo Nicaragüense de Ciencia y Tecnología (Conicyt) desarrolló un marco jurídico. Entre las leyes trabajadas se encuentran la Ley de protección de datos personales, Ley especial de delitos informáticos y la Ley de firma electrónica. Radoykov puso a la disposición la experiencia de la UNESCO en este campo, para compartir las buenas prácticas que existen en otros países y ver si se puede completar, agregar, en el marco del mandato de la UNESCO.

Manifestó que, además, se están preparando principios directores y orientaciones sobre el establecimiento de políticas nacionales de la información.

"Lo que es importante es demostrar la voluntad a nivel nacional de apoyar el desarrollo de la sociedad de la información, porque sin esta voluntad política es muy difícil llegar a resultados concretos", añadió el especialista.

Consideró que hay también aspectos éticos que se preservan gracias a estas leyes y aspectos de desarrollo de diferentes tipos de acciones para sostener la sociedad de la información a nivel nacional con todos sus actores.

ESPERAN PROYECTOS

En relación al financiamiento de proyectos, Radoykov dijo que la UNESCO trabaja en el marco de "Información para todos", y en este momento están esperando los proyectos concretos que Nicaragua pueda presentar en el marco de este programa, para poder empezar con el financiamiento al menos de un proyecto. Estos deben ser presentados antes del 15 de febrero de este año[∝].

Arlen Pérez

[∝] www.laprensa.com.ni