REPÚBLICA DE CUBA
UNIVERSIDAD DE SANCTI SPIRITUS
JOSÉ MARTÍ PÉREZ
FACULTAD DE HUMANIDADES

Título: Propuesta de modificaciones al tratamiento legal que reciben las conductas delictivas generadas por la criminalidad informática en Cuba

Autor: Mijail Valdivia Chernoziomova

Sancti Spíritus
2011

Resumen

El creciente desarrollo tecnológico que cada día experimenta la sociedad posibilita la comisión de nuevas formas delictivas, para lo cual en muchas ocasiones los sistemas de la administración de justicia no se encuentran preparados. Nuestro país no se halla ajeno a esta situación por lo que el presente trabajo versa sobre el tratamiento legal que recibe la criminalidad informática, pretendiendo con él contribuir a su perfeccionamiento en cuanto al análisis de las conductas delictivas que provocan este fenómeno, dado que no se puede hablar de delito informático si no está previamente sancionado en una norma penal.

La tesis en su estructura cuenta con tres capítulos en los cuales se realiza un análisis de las características de la citada criminalidad, el marco histórico en el que se ha desenvuelto, las definiciones y conceptos que se han dado al respecto por los juristas nacionales y de otras latitudes, así como las principales tipicidades. Además se expone la regulación jurídica en el Derecho Comparado, en la que se abordan las figuras delictivas específicas que reprimen y sancionan estos delitos.

Finalmente se analizan las tipicidades contentivas en el Código Penal que guardan estrecha relación con la criminalidad informática, a fin de dar una propuesta de modificaciones, que permita rediseñar el tratamiento legal a la misma.

Abstract

The growing technological development that every day experiences the society facilitates the commission in new criminal ways, for that which in many occasions the systems of the administration of justice are not prepared. Our country is not unaware to this situation for what the present work turns on the legal treatment that receives the computer crime rate, seeking with him to contribute to its improvement as for the analysis of the criminal behaviours that cause this phenomenon, since one cannot speak of computer crime if it is not previously sanctioned in a penal norm.

The thesis in its structure has three chapters in which it is carried out an analysis of the characteristics of the mentioned crime rate, the historical mark in the one that has been unwrapped, the definitions and concepts that have been given in this respect for the national jurists and of other latitudes, as well as the main tipicidades. Also these regulations as well exposed in the Compared Right, in the specific criminal figures are approached, which repress and they sanction these crimes.

Finally the criminal figures are analyzed in the Penal Code that keep narrow relationship with the computer crime rate, in order to give a proposal of modifications that allows redrawing the legal treatment to the same one.

Índice

Introducción

El desarrollo de las Tecnologías de la Informática y las Comunicaciones en los últimos tiempos ha progresado de forma acelerada. Su influencia en la industria, los servicios, las comunicaciones, la carrera armamentista, la salud, entre otros aspectos de la economía mundial es sumamente elevada, aumentando cada día, tanto en nivel de especialización como en dependencia de los sectores de la sociedad en su uso.

Las Tecnologías de la Informática abren nuevos y versátiles caminos que imponen con premura la realización de cambios en pos del desarrollo de una cultura informática dirigida a elevar cada día las medidas de seguridad y el control de los servicios que se brindan o explotan.

La constante evolución y la alta demanda de adquirir tecnologías, ha traído como consecuencia la aparición de nuevas formas delictivas, por lo que internacionalmente se ha comenzado a hablar de crimen informático o delitos donde interviene el uso de los medios informáticos, siendo así el tema que se propone. Este tiene gran importancia, principalmente para el Sistema de Justicia Penal ya que conocer los elementos característicos que genera dicha acción prepara para la investigación y procesamiento de estas conductas, que están incidiendo en la mayoría de los sectores fundamentales de la economía y la sociedad cubana.

El fenómeno no es nuevo, ha estado presente en casi todos los países desarrollados y en muchos de los del tercer mundo, lo que se está incrementando con el avance de la tecnología; siendo este uno de los problemas a los que se enfrenta el país hoy en día. El citado avance de toda esta infraestructura en las comunicaciones, informaciones y negocios, se ve muy compenetrado con las actividades políticas, culturales y comerciales de la nación, propiciando que el área dedicada a la informática de las organizaciones estatales gane cada día más espacio.

Es significativo además que las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave,

estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la propiedad o la dignidad de los individuos o el interés público.

Estas nuevas herramientas son usadas por personas, que por su naturaleza humana suelen enfrentarse a situaciones que se alejan de un claro comportamiento de convivencia en sociedad, con acciones que se utilizan para sí y al aporte de las nuevas técnicas de la criminalidad.

Las mencionadas acciones perturbadoras de la convivencia social que han nacido al amparo de estas herramientas tecnológicas en el ámbito mundial, han generado un cambio en la percepción sobre la seguridad informática, la que se ha ido desarrollando muy por detrás de la realidad del alcance de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de la necesidad de control por parte de los organismos encargados de ello.

Las experiencias obtenidas por Cuba, por la Organización de las Naciones Unidas, en la Comunidad Europea, en los Estados Unidos y en otros países; han inducido a la necesidad de crear los organismos requeridos para enfrentar el problema del delito, siendo un hecho grave que requiere de urgentes medidas de todo tipo tanto en el ámbito legislativo, como el de las tecnologías y su socialización.

En los momentos actuales en el país se carece de un tratamiento legal a las conductas delictivas que generan la criminalidad informática, debido a que el Código Penal por tener más de veinte años de vigencia, no contempló el uso de las Tecnologías de la Informática y las Comunicaciones para cometer delito. Esto a causa de que el desarrollo del país en los momentos en que se dictó el citado código no posibilitaba ampliamente el uso de estos medios y por tanto no existían elementos suficientes para contemplar estas manifestaciones. Hasta ahora se han tipificado estas acciones por delitos tradicionales, aunque no siempre se obtienen los resultados esperados, dado que no se puede hablar de delito informático si no se encuentra plasmado en una norma penal.

Considerando todo lo anterior se plantea el siguiente **Problema científico:** ¿Cómo proponer modificaciones al tratamiento legal que reciben las conductas delictivas que generan la criminalidad informática en Cuba, para poder incrementar su efectividad?

Para la solución de este problema se plantea la siguiente **hipótesis:**

Se podrá incrementar la efectividad del tratamiento legal que reciben las conductas delictivas que generan la criminalidad informática en Cuba realizando modificaciones a la normativa actual y a las posibles afectaciones a determinados bienes jurídicos.

Como variables se definen las siguientes:

- **Variable independiente:** Conductas delictivas, son las que propician la aparición de la criminalidad informática generando la causa del problema.
- **Variable dependiente:** Tratamiento legal, es el efecto que se genera para darle tratamiento a las acciones delictivas.

Para estructurar la investigación y responder a la problemática científica planteada se propone el siguiente **objetivo general:**

- Valorar el tratamiento legal que reciben las conductas delictivas que generan la criminalidad informática en Cuba para proponerle modificaciones e incrementar su efectividad.

Como **objetivos específicos** de la investigación se encuentran los siguientes:

1. Exponer los fundamentos teóricos y jurídicos de la criminalidad informática a nivel internacional y nacional, para establecer sus elementos característicos, generadores, conceptuales y criminológicos.
2. Analizar la legislación que reprime las manifestaciones de la criminalidad informática en el Derecho Comparado y su estado actual, para caracterizar generalidades y especificidades, fortalezas y vulnerabilidades.
3. Analizar la normativa nacional y sus principales objetividades jurídicas en el Código Penal que guardan estrecha relación con el uso de los medios informáticos y la seguridad informática, para definir criterios que permitan modificar su tratamiento legislativo.

La investigación permite:

1. Demostrar la insuficiencia que presenta la legislación nacional para darle tratamiento a las conductas que generan la criminalidad informática.
2. Fundamentar criterios teóricos, metodológicos y jurídicos que posibiliten modificar el tratamiento legislativo que reciben las conductas delictivas generadas por la criminalidad informática.

Se emplearon como **métodos y técnicas**:

- Teórico-Jurídico: Para la exposición de los fundamentos generales sobre el tema, con especial énfasis en los conceptos y clasificaciones del mismo.
- Histórico-Lógico: Para el análisis de los principales antecedentes históricos y legales sobre el delito informático, haciendo especial referencia a su desarrollo internacional y nacional.
- Derecho Comparado: Para analizar y evaluar la forma y tratamiento legal que se le da a esta figura delictiva en el marco internacional.
- Exegético-Analítico: Para valorar la regulación y desarrollo actual sobre la materia objeto de la investigación, establecer los principales elementos del delito, sus posibles manifestaciones y características.
- Análisis y síntesis: Para a través del estudio, llegar a alcanzar una visión del fenómeno, que propicie su contextualización y una mejor comprensión del tratamiento legal que recibe.

Y como técnicas:

- Revisión bibliográfica: Para la detección de información actualizada de corte teórico-doctrinal sobre el tema objeto de estudio.
- Análisis de estadística: Para evaluar el comportamiento de las manifestaciones delictivas donde intervengan las tecnologías en el territorio de la provincia de Sancti Spíritus.
- Revisión de Causas Penales: Para determinar el grado de efectividad y características de las medidas adoptadas, con el fin de minimizar los riesgos y vulnerabilidades que generan la criminalidad informática.

La tesis se estructura en tres capítulos, de la siguiente forma:

Capítulo 1: Fundamentos teóricos y jurídicos de la criminalidad informática.

En el mismo se exponen los fundamentos teóricos y jurídicos de la criminalidad informática para establecer sus elementos característicos y generadores, se estudian los determinantes criminógenos y los factores que conllevan a que el hombre cometa el delito; así como su surgimiento, desarrollo y perspectiva en que se ha desenvuelto dicha manifestación y las principales tipicidades y objetividad jurídica que afectan la misma.

Capítulo 2: Análisis de la regulación jurídica del Derecho Comparado sobre la criminalidad informática.

En el se analiza la normativa del Derecho Comparado y su estado actual para determinar los principales elementos que la protegen y como se comporta, lo que permite establecer generalidades y especificidades, fortalezas y vulnerabilidades.

Capítulo 3: Propuesta de modificaciones al tratamiento legal de la criminalidad informática en Cuba.

El capítulo analiza los fundamentos jurídicos y normativos en Cuba, sobre las conductas delictivas que generan la criminalidad informática y en el se proponen las modificaciones al tratamiento legal que recibe la misma.

Capitulo 1: Fundamentos teóricos y jurídicos de la criminalidad informática.

1.1 – Marco teórico y jurídico de la criminalidad informática.

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar tanto a la diversificación de los delitos tradicionales, como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no la criminalidad informática y con ello los delitos informáticos del resto.

1.1.1 - Concepto o definición de criminalidad o delito informático en el Derecho Comparado y en Cuba.

La criminalidad informática se caracteriza por ser una conducta ilícita y antisocial donde se involucran las Tecnologías de la Informática y las Comunicaciones como método, medio o fin, todo ello va aparejado a que al ocurrir se genera el delito informático.

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

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como: robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje y otros. Sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del Derecho.

Para CARLOS SARZANA[1], 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, o como mero símbolo".

LIDIA CALLEGARI[2] define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Para el abogado chileno RODOLFO HERRERA BRAVO[3], el delito informático es la "acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software de un sistema de tratamiento automatizado de la información".

RAFAEL FERNÁNDEZ CALVO[4] 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 definidos en el Título 1 de la Constitución Española".

MARÍA DE LA LUZ LIMA[5] dice que el delito electrónico en un sentido amplio, "es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

JULIO TÉLLEZ VALDÉS[6] conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se

---

[1] SARZANA, CARLOS. Criminalita e Tecnología en Computers Crime; Rassagna Penitenziaria e Criminología. Nos. 1-2 Año 1. Italia. Roma. p. 53.

[2] CALLEGARI, LIDIA. Delitos informáticos y legislación. Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. No. 70 julio-agosto-septiembre. Colombia. Medellín. 1985. p.115.

[3] HERRERA BRAVO, RODOLFO. Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley Chilena No. 19. 223. Chile. Santiago de Chile. 2003. p. 76.

[4] FERNÁNDEZ CALVO, RAFAEL. El tratamiento del llamado "delito informático" en el proyecto de ley Orgánico del Código Penal; reflexiones y propuestas de la CLI "Comisión de Libertades e Informática" en Informática y Derecho. p.1150.

[5] LIMA DE LA LUZ, MARÍA. Delitos Electrónicos en Criminalia. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio. México. 1984. p.100.

[6] TÉLLEZ VALDÉS, JULIO. Derecho Informático. Instituto de Investigaciones Jurídicas. Ed. Mc Graw Hill. Interamericana de México S.A. México. 1997. p. 103 - 104.

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".

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como abarcadora y lo define como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos". En cuanto a la Comisión Europea, se centró en un concepto amplio de "delito informático" al indicar que es cualquier delito que de alguna manera implique el uso de la tecnología de la información.

La Organización de Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Tratamiento al Delincuente, celebrado del 27 de agosto al 7 de septiembre de 1990 en La Habana Cuba, estableció que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos[7].

En nuestro país no se ha llegado a establecer la definición de delitos informáticos siendo la mayor tendencia a adoptar definiciones de estudiosos de otras latitudes, no obstante a eso, juristas cubanos han llegado a formular sus propios conceptos.

Al respecto YARINA AMOROSO FERNÁNDEZ[8] plantea que el delito informático "es el conjunto de acciones u omisiones que se pueden desatar, por sobre los medios informáticos utilizados para realizar conductas delictivas que tienen su incidencia en la naturaleza de los bienes atacados, la forma de realización y los daños que pueden provocar".

ALEJANDRO GARCÍA GARCÍA[9] establece que el delito informático es "toda conducta con características delictivas, es decir, sea antijurídica y culpable que atenta contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o

---

[7] Naciones Unidas. Revista Internacional de Política Criminal. Nos. 43 y 44. Naciones Unidas. Nueva York. 1994. p. 50.

[8] AMOROSO FERNÁNDEZ, YARINA. "La Informática como objeto de Derecho". Revista Cubana de Derecho. No. 1. Cuba. 1991. p. 45.

[9] GARCÍA GARCÍA, ALEJANDRO. Informática Jurídica y Derecho Informático. Cuba. 2006. p. 11.

datos, a través del empleo de las tecnologías de la información y que se distinga de los delitos computacionales o tradicionales informatizados".

Para ENRIQUE CORDOVÉS RODRÍGUEZ[10] son "todos los actos ilícitos ejecutados de cualquier forma por una persona natural o jurídica no autorizada, a dar, obtener, crear, destruir, modificar, o de cualquier forma manipular las nuevas tecnologías de las comunicaciones o la informática en beneficio propio o de un tercero".

Se debe destacar que en Cuba existen tres criterios[11] para darle respuesta a los delitos donde intervienen las tecnologías, así lo ha establecido el jurista cubano antes mencionado, dentro de los que se encuentran:

- **Los delitos tradicionales:** Este criterio establece que los delitos informáticos no existen, solo son la manifestación de las tipicidades que constan en nuestro ordenamiento jurídico pero con un nuevo modus operandis.
- **Los delitos informáticos:** Que es una nueva forma de conducta, que los delitos tradicionales no le dan la respuesta debida.
- **Mixto:** Se puede tener en cuenta ambas posiciones a partir de las conductas que solo deben ser adaptadas dentro de los delitos tradicionales y otras conductas que no poseen la respuesta jurídica conforme al derecho, por lo que hay que tipificarlas.

Respecto a las definiciones y conceptos que se han dado en el contexto internacional y nacional; hay que destacar que esta tipicidad se origina de la conducta llevada a cabo por él o los grupos de individuos, sean personas naturales o jurídicas; donde están implícitas las Tecnologías de la Informática y las Comunicaciones como ente principal; ya que sin ellas no habría forma de cometer el delito.

Por otra parte las mencionadas tecnologías se utilizan como medio para cometer la acción o fin para llevarla a cabo, teniendo como resultado una afectación económica,

---

[10] CORDOVÉS RODRÍGUEZ, ENRIQUE. Definiciones sobre Delito Informático. Intranet MININT \ Web Delitos informáticos\ ismi.htm. Cuba. 2007.

[11] CORDOVÉS RODRÍGUEZ, ENRIQUE. Características Generales de la Criminalidad Informática en Cuba. Cuba. Ciudad de La Habana. 2006. p. 3.

social o personal. En ello el delito tiene que estar contemplado dentro de la norma penal con figuras delictivas propias, con la función de reprimir y proteger esa objetividad jurídica; que de no ser así se hablaría de criminalidad informática o delito donde intervienen las Tecnologías de la Informática y las Comunicaciones, pero no de delito informático.

1.1.2 - Principales características de la criminalidad informática.

La criminalidad informática en general presenta características propias que generan estos tipos delictivos, según lo establecido por JULIO TÉLLEZ VALDÉS[12]:

- Son conductas criminales de cuello blanco puesto que sólo un determinado número de personas con ciertos conocimientos técnicos pueden llegar a cometerlas.
- Son acciones ocupacionales, dado a que muchas veces se realizan cuando el sujeto se halla trabajando, por las características técnicas de su labor y la presencia y el acceso al equipamiento que propicia los elementos necesarios para hacer uso de los mismos.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, debido a que en muchas ocasiones se realizan con el objetivo de producir beneficios monetarios por parte de los autores directos o en beneficio de otros, o su simple comisión propicia cuantiosas pérdidas.
- Ofrecen posibilidades de rapidez y acercamiento en tiempo y espacio. Un delito cometido a través de las Tecnologías de la Informática y las Comunicaciones puede ser realizado con gran celeridad, en apenas décimas de segundo y sin una necesaria presencia física, como son los casos de la activación de un virus informático o el robo de información mediante máquinas inteligentes. Respecto al

[12] Ídem 6.

espacio territorial puede ser cometido a miles de kilómetros por el uso de las redes de telecomunicación como Internet.

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho y el déficit de preparación y control de quienes investigan y combaten estos hechos.
- Favorecen la especialización técnica de los autores. La complejidad propia de las tecnologías implica un alto nivel de conocimientos, respecto a su manejo y estructura, que han de tener los autores, en términos generales para que puedan cometer los delitos de este tipo.
- Propician la facilidad para encubrir el hecho y borrar las pruebas lo que provoca que presenten grandes dificultades para su comprobación, debido a la naturaleza de la tecnología digital. Es factible para un sujeto experimentado, borrar o destruir las huellas o alteraciones que haya podido causar en un sistema informático, eliminando así las pruebas que le incriminen.
- Pueden ser imprudenciales y no cometidas con intención, puesto que la mala manipulación de la tecnología por falta de conocimientos técnicos y operacionales puede originar como consecuencia la destrucción, modificación o pérdidas de datos e informaciones.
- Tienden a proliferar cada vez más, dado que el desarrollo tecnológico y la facilidad de su alcance y manipulación propician un aumento en su comisión.
- Son ilícitos e impunes de manera manifiesta ante la ley, dado que en muchas ocasiones su radicación se limita a tomar medidas administrativas sin prever el alcance y la magnitud del delito cometido.

Debido a las características descritas de estos delitos[13], se plantean los siguientes problemas que dificultan que pueda ser perseguible en la práctica:

1. La determinación del sujeto, dado que en ocasiones se puede definir el ordenador concreto desde el que se ha cometido un hecho delictivo pero no quién lo materializó. El hecho de que una pluralidad de personas tengan acceso al mismo hace difícil la determinación del autor material del ilícito, debiendo

[13] Ídem 10.

acudir a sistemas de prueba tradicionales para esta finalidad: testigos, registros de entrada en el local entre otros que no siempre son posibles.

2. La facilidad para ocultar pruebas o indicios, tal y como se expresa anteriormente. La posibilidad de destruir los registros informáticos u otros indicios digitales de un delito informático por una persona con los conocimientos necesarios puede dificultar enormemente la prueba de dicho hecho.
3. La complejidad técnica de estos tipos delictivos generalmente son cometidos por expertos en informática y telecomunicaciones. Por ello es necesario un alto grado de preparación por parte de las autoridades que persigan y conozcan de estos hechos o de sus colaboradores.
4. La conexión de causalidad, dado que hay un distanciamiento en el espacio e incluso en el tiempo entre el acto delictivo y el resultado pernicioso. Es necesario probar la relación de causalidad entre ambos sucesos. Se debe conectar el hecho producido por el actor con el perjuicio cometido; en algunos casos a miles de kilómetros de allí.
5. El lugar de comisión del delito. En el caso de Internet donde el delito, la legislación y la jurisdicción competentes no siempre coinciden en el mismo lugar. Por ejemplo, la entrada de un hacker desde un determinado país a un servidor de correo en cualquier otro.

Además de lo anterior los delitos informáticos se pueden clasificar en dos tipos: por un lado, los delitos clásicos que ahora pueden ser cometidos también a través de las tecnologías, y por otro lado, los nuevos delitos surgidos específicamente con ocasión de la informática y de la telemática[14].

1.2 – Análisis criminógeno de la criminalidad informática.

Una de las principales características de los delitos informáticos es su elevado nivel de tecnicidad, con clara incidencia en el ámbito probatorio, hecho que provoca una alta probabilidad de impunidad en su esfera y que no deriva exclusivamente de las dificultades probatorias que pueden generar conductas como ésta.

[14] Ibídem 10.

La doctrina ya parece haber dejado de lado la pretensión de encontrar una explicación de corte criminológico a la delincuencia informática y por el contrario, parece vislumbrarse que el "*computer crime*" (crimen informático) aparece mayoritariamente como una modalidad de delincuencia ocupacional. Al respecto se ha señalado: "Las empresas deben tener en cuenta el hecho que la mayor parte de la criminalidad informática es cometida por sus empleados"[15]. De la misma forma, las Naciones Unidas en investigaciones realizadas plantea que el 90% de los delitos informáticos son ejecutados por empleados de las empresas o instituciones afectadas[16].

No obstante teóricos de la materia dentro de ellos los doctores JULIO TÉLLEZ VALDÉS[17] y MARÍA LUZ LIMA[18] sostienen que las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Dentro de ellos los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral 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.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que la diferencia entre ellos es la naturaleza de los delitos 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 informático es tema de divergencias ya que para algunos no es indicador de delincuencia, en tanto que otros aducen que los autores son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico; características que pudieran encontrarse en un empleado de un sector de procesamiento de datos.

---

[15] REYNA ALFARO, LUIS M. Aproximaciones victimológicas al Delito Informático. Capítulo Criminológico. Vol. 31. Nº 4. 93-104ISSN: 0798-9598. Universidad de San Martín de Porres. Universidad Nacional Mayor de San Marcos. Perú. Lima. Octubre-Diciembre 2003. p. 5.
[16] Vid. http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml. 2011.
[17] Ibídem 6.
[18] Ídem 5.

Sin embargo, teniendo en cuenta los rasgos ya mencionados de las personas que cometen los delitos informáticos, algunos estudiosos de la materia los han catalogado como delitos de cuello blanco, término introducido por primera vez por el criminólogo norteamericano EDWIN SUTHERLAND[19] en el año 1943.

Este conocido criminólogo señala que un sin número de conductas consideradas como delitos de cuello blanco, aún no están tipificadas en los ordenamientos jurídicos como delitos, entre ellas las violaciones a las leyes de patentes y fábricas de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios.

Asimismo, el citado autor plantea que tanto la definición de los delitos informáticos como los de cuello blanco, no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino en correspondencia al sujeto activo que los comete. Entre las características en común que poseen ambos se tiene que el sujeto activo 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.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La cifra negra es muy alta, no es fácil descubrirlo y sancionarlo; en razón del poder económico de quienes lo cometen lo que genera daños altísimos. Existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad. Esta 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 ilícitos se consideran a sí mismos personas respetables. Otra coincidencia que tienen estos tipos de delitos es que generalmente son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Se tiene que distinguir que el 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 o

[19] SUTHERLAND, EDWIN. Teoría de la Criminología. Estados Unidos de América. Washington. 1943. p. 10.

gobiernos; que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante para el estudio de los delitos informáticos, ya que mediante él se pueden conocer los diferentes ilícitos que cometen los delincuentes informáticos, con el objeto de prever las acciones antes mencionadas; debido a que muchas de las acciones son descubiertas casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Por otra parte se debe reconocer que en muchas ocasiones el sujeto pasivo del delito no es conciente de que sobre el se ha cometido una conducta ilícita, ya que el sujeto activo aprovecha la brecha del desconocimiento para cometer estas fechorías. Al momento de ser descubierto, el factor tiempo ha conspirado en que se dificulte su investigación y procesamiento.

Dado lo anteriormente mencionado, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los hechos no son descubiertos 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; 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 entidad 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.

Asimismo, se puede admitir que se han elaborado clasificaciones sobre los agentes que intervienen sobre las Tecnologías de la Informática y las Comunicaciones para cometer delitos posibilitando que se puedan reconocer con una mayor efectividad, dentro de los que se encuentran, según CLAUDIO HERNÁNDEZ[20].

Hackers: En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender

[20] HERNÁNDEZ, CLAUDIO. “Hackers” Los piratas del Chip y de Internet. Ed. Mc Graw Hill. México. 2001. p. 101.

sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de que he estado aquí, pero no modifican ni se llevan nada del ordenador atacado.

Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de virus o crack de un software o sistema informático.

Crackers: Es el hacker fascinado por la capacidad para romper la entrada a sistemas y software y que se dedica única y exclusivamente a este perfil. Este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la red para conocimientos de otros, en esto comparten la idea y la filosofía de los hackers.

En la actualidad es habitual ver como se muestran los cracks[21] de la mayoría de software de forma gratuita a través de Internet. El motivo de que estos cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.

Lamers: Son individuos con ganas de hacer hacking, pero que carecen de cualquier conocimiento; apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar. Normalmente la posibilidad de entrar en otro sistema remoto o girar un gráfico en la pantalla de otro ordenador, le fascinan enormemente.

Este es quizás el grupo que más peligro acontece en la red ya que ponen en práctica todo el software de hackeo que encuentran. Así es fácil ver como un lamer prueba a

[21] **Cracks:** Código o serie de códigos que se utiliza para penetrar sistemas y programas con el objetivo de tener el control de los mismos y poderlos utilizar según sus posibilidades y fines.

diestro y siniestro un bombeador de correo electrónico[22] o un Sniffers[23] auto denominándose así hacker.

Copyhackers: Es conocido en el terreno del crackeo de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Emplean la ingeniería social para convencer y entablar amistad con los verdaderos hackers, les copian los métodos de ruptura y después se los venden a los bucaneros. Poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello extraen información del verdadero hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

Bucaneros: Son peores que los lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los copyhackers. Sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos crackeados pasan a denominarse "piratas informáticos" así puestas las cosas, es simplemente un comerciante, el cual no tiene escrúpulos a la hora de explotar un producto de cracking a un nivel masivo.

Phreaker: Este grupo es bien conocido en la red por sus conocimientos profundos en telefonía, tanto terrestre como móvil. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su proceso de datos.

Newbie: Es un novato que navega por Internet, tropieza con una página de hacking y descubre que existe un área de descarga de buenos programas de hackeo. Después baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los

[22] Programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar.
[23] Programa para controlar la red, interceptando contraseñas y correos electrónicos enviando varios mensajes, con dirección falsa amenazando un sistema.

lamers, los newbies aprenden el hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

Trashing: Son los individuos que tienen como propósito la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa o una entidad, con el fin de utilizarlo en los medios informáticos en actividades delictivas.

Script Kiddie: Denominados skid kiddie o script kiddie, son el último eslabón de los clanes de la red. Son simples usuarios de Internet, sin conocimientos sobre hack o el crack en su estado puro, devotos de estos temas, pero no los comprenden. Se limitan a recopilar información y buscar programas de hacking y después los ejecutan sin leer primero los ficheros "*Readme*" de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos su propio ordenador. Esta forma de actuar, es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de hacking. Podrían llamarse los pulsa botones de la red.

1.3 - Marco histórico en el que se ha desenvuelto la criminalidad informática y su prevención a nivel internacional y nacional.

La sociedad en su devenir histórico siempre ha estado caracterizada por su constante evolución, siendo así que la tecnología desde momentos inmemorables también a dado su aporte al desarrollo humano, en los momentos actuales las Tecnologías de la Informática y las Comunicaciones también están en constante desarrollo y perfeccionamiento, es tan rápido que las sociedades muchas veces no son capaces de adaptarse y estar preparadas para estos nuevos cambios que se originan o no son capaces de seguirlos en su plenitud; ejemplo de esto son los países del tercer mundo.

Desde el período comprendido entre 1938 y 1952[24] era característico el gran desconocimiento de las capacidades de las computadoras, así lo confirma un estudio realizado en esta época que determinó que con veinte computadoras se saturaría el

[24] Máquinas basadas en válvulas al vacío, con 18 000 tubos, 70 mil resistencias, 7 500 interruptores, consumía 200 Kw. de energía requiriendo todo un sistema de aire acondicionado, tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo.

mercado de los Estados Unidos en el campo del procesamiento de datos[25]. (Ver Anexo 1).

A comienzo de la década de 1950[26] surge un elemento muy importante “el software”, el cual comienza a tratar de alcanzar el paso del hardware; apareciendo así el usuario de las computadoras que va cambiando y evolucionando con el tiempo. De estar totalmente desconectado a ellas en las máquinas grandes pasa a la PC (*Personal Computer*) a ser pieza clave en el diseño tanto del hardware como del software, respecto a este último se inicia una verdadera carrera para encontrar la manera en que el usuario pase menos tiempo capacitándose y entrenándose y más tiempo produciendo.

En esta época las primeras manifestaciones aparecen por un grupo de alumnos prestigiosos del Massachussets Institute of Technology (MIT) quienes fueron los primeros en darse el calificativo de hackers que en 1959 apuntaron al primer curso de programación que el instituto ofreció a sus alumnos, haciendo uso de los ordenares que eran aparatos demasiados costosos que ocupaban salas enteras; estos comenzaron a introducir directamente programas para tener tanto contacto y control como les fuera posible con el ordenador, no les suponía ningún problema el usarlo desde una sala de terminales a la que en realidad no tenían acceso de modo oficial colocándose en ellas por la noche[27]. La contribución mas importante de este grupo no fue la de adoptar este término sino la de ser los primeros en pensar diferente acerca de cómo se usaban los ordenadores y lo que podían hacer con ellos.

En esta etapa la Agencia de Proyectos de Investigación Avanzada (ARPA) se inició en el Departamento de Defensa de los Estados Unidos para investigar los campos de la ciencia y la tecnología militar. El objetivo de la propuesta era plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo. Se suponía que una red de comunicaciones, por si misma, no es fiable debido a que parte de ella podría ser

[25] Ídem 19.
[26] Máquinas construidas con circuitos de transistores, se programan en nuevos lenguajes llamados de alto nivel.
[27] Ibídem 19.

destruida durante un ataque bélico[28], teniendo como resultado posteriormente el surgimiento y desarrollo de Internet.

En estos años predominaba el desconocimiento de los ordenadores ya que esta tecnología estaba revolucionándose y los principales esfuerzos se destinaban al desarrollo de la misma y creación de nuevas bases para la comunicación.

En 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación, planteando que las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos. En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Tratamiento al Delincuente, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos[29].

---

[28] TOLEDO DUMENES, JOSÉ ALFONSO. Delitos emergentes en Internet y el desafío de los carabineros de chile en la prevención y control en la era informática. Chile. 2007. p. 8.

[29] Ídem 7.

En 1992 la Asociación Internacional de Derecho Penal durante el coloquio celebrado en Werzburgo, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad". Se elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos[30].

En 1995 es fundada la International Organization on Computer Evidence (IOCE) durante la II Conferencia Internacional para la Evidencia Computacional. Tiene como objetivo propiciar un foro internacional de intercambio de información entre agencias del orden relativo a la investigación forense de computadoras. Ha efectuado cuatro Conferencias Internacionales y publicado numerosos procedimientos y documentos relacionados con todos los aspectos de la evidencia computacional. Estableció seis principios y cuatro definiciones especialmente escritos para la evidencia digital que fueron adoptados por el Grupo de los Ocho (G8)[31].

En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como: aplicaciones en la administración de las tecnologías informáticas / cibernéticas, blanqueo de capitales, contrabando y narcotráfico hacia una policía Europea en la persecución del delito cibernético. Internet: a la búsqueda de un entorno seguro[32].

En marzo de 1998, la IOCE fue designada para trazar principios internacionales en los procedimientos relativos a la evidencia digital y garantizar la armonización de métodos

[30] ESTRADA GARAVILLA, MIGUEL. Delitos Informáticos. http://www.universidadabierta.edu.mex. Universidad Abierta. México. 2008. p. 16.
[31] Ídem 28.
[32] Ibídem 28.

y practicas entre países. También debían posibilitar el uso de evidencia digital recolectada por un estado en la corte de otro estado[33].

La organización Antivirus Test, que presta servicios de prueba y consultoría a empresas de seguridad informática, calcula que a inicios de 2008 había un total de 9 millones de piezas de malware[34], o software maliciosos en el mundo. A mediados de 2009 la empresa ya registraba 22 millones, sólo de esta amenaza.

Desde 2001 el terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios u oficinas oficiales.

La cantidad de amenazas informáticas detectadas en el 2010 en la red ha aumentado cerca de 1700% en dos años, entre enero de 2005 y diciembre de 2007; el peligro de navegar y realizar transacciones se ha hecho 17 veces más grande desde 2006[35]. En el 2008 las alarmas sobre el incremento de la peligrosidad en Internet se dispararon y continuaron encendidas a lo largo de este año.

En los momentos actuales (2011) ya se manejan términos como las ciberguerras, al igual que sucede en las guerras del mundo real, no hay bandos con uniformes en el que se puede distinguir a los distintos combatientes. Se habla de lucha de guerrillas, donde no se sabe quién es el que ataca, ni desde dónde lo hace, lo único que puede tratar de deducirse es el fin con el que lo hace. Otra novedad se considera la ciberprotesta[36] o ciberactivismo, donde muchos países están intentado regular legislativamente este tipo de actuaciones rápidamente, para poder ser considerada esta actividad un delito y, por lo tanto, perseguida y condenable. Se consolida también la ingeniería social con el incremento de la comunicación mediante las redes de acceso global donde se fortalecen como herramientas para los hackers[37].

---

[33] ACURIO DEL PINO, SANTIAGO. Dr. Delitos Informáticos: Generalidades. Profesor de Derecho Informático de la PUCE. España. 2007. p. 40.
[34] **Malware:** Por sus siglas en inglés, denominación que se les da a los códigos maliciosos.
[35] Vid. http://www.belt.es. 2011.
[36] **Ciberprotesta:** Acción y efecto de protestar haciendo uso de los medios telemáticos y las posibilidades que estos brindan.
[37] Vid. http://www.cucert.cu. Cuba. 2011.

En Cuba la incidencia comenzó muy incipientemente en el año 1995, detectándose algunos casos aislados y observándose por primera vez la ocurrencia, en los delitos tradicionales, de la utilización de la tecnología para la comisión de los hechos delictivos. Esta forma de conducta delictiva se comenzó a trabajar de forma especializada y hasta la fecha se han trabajado un número reservado de hechos en los que ha estado presente las TIC[38].

En noviembre de 1996 con el desarrollo obtenido, el país necesitó establecer medidas de seguridad y protección en los organismos para evitar las posibles sustracciones de información, evitar los piratas informáticos, o la destrucción de la información, acciones comunes que se realizan en otros países.

Para ello el MININT promulgó la Resolución No. 6 de 1996 que es el Reglamento sobre la Seguridad Informática, Seguridad de Operaciones y trabajos con redes de alcance global, también se pone en vigor el Decreto Ley 209 de 1996 mediante el cual surge la Comisión Interministerial para la atención de todos los asuntos relacionados con el acceso del país a redes informáticas de alcance global, como Internet, en noviembre de 1999, cuando se pone en vigor el Decreto Ley 199 de 1999 sobre la Seguridad y Protección de la Información Oficial, en dicha normativa en su capítulo séptimo, los artículos del 43 al 49 tratan sobre la seguridad informática.

En el año 2000 se creó el Ministerio de la Informática y las Comunicaciones, donde el antiguo Ministerio de las Comunicaciones desapareció. Se unió y centralizó todo lo relacionado con la informática en estrecha relación con las comunicaciones.

Actualmente se encuentra vigente la Resolución No. 127 de 2007[39] de fecha 24 de julio, del Ministerio de la Informática y las Comunicaciones (MIC), que puso en vigor el "Reglamento de Seguridad para las Tecnologías de la Información", y su objetivo es establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Este nuevo reglamento aporta una

[38] CORDOVÉS RODRÍGUEZ, ENRIQUE. Manual de Enfrentamiento a la Criminalidad Informática. Cuba. 2004. p. 10.
[39] Vid. Gaceta Oficial No. 057 Ordinaria de 30 de agosto de 2007. Cuba.

serie de elementos superiores al anterior, si se tiene en cuenta que se incluyen varias conductas novedosas que no llegan a constituir delito pero que requieren de atención administrativa y laboral.

El fenómeno de la criminalidad informática en nuestro país se ha comportado con sus propias características, el incremento en pocos años es significativo, esto lo demuestra el trabajo pericial desarrollado por la Sección de Informática Criminalística que entre los años 1995 y 1998[40], trabajó pocos casos, con sólo 153 evidencias, pero del año 1999 al 2003 aumentó la cifra de solicitudes periciales considerablemente, obteniéndose más de 1200 evidencias con más de 1800 huellas reveladas.

1.4 – Principales tipicidades de la criminalidad informática.

El estudio de la criminalidad informática plantea que en el delito informático hay que distinguir el medio y el fin, para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delito, el medio por el que se comete debe ser un elemento, bien o servicio patrimonial del ámbito de la responsabilidad de la informática y la telemática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero. Asimismo JULIO TÉLLEZ VALDÉS[41] clasifica a estos delitos de acuerdo a dos criterios:

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.
c. Planeamiento y simulación de delitos convencionales (robo, 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.

[40] Ídem 38.
[41] Ibídem 6.

g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria ficticia.
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.

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, dentro de los que se puede mencionar:

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
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 un rescate, etc.).

Por otra parte, existen diversas manifestaciones que pueden ser cometidas y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- **Acceso no autorizado:** Uso ilegítimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

- **Infracción al copyright**[42] **de bases de datos**: Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de correos electrónicos**: Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de manifestaciones tales como:

- **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 en el ámbito internacional.
- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Las conductas lesivas a la información planteadas según el Consejo de Europa y el XV Congreso Internacional de Derecho[43] son las siguientes:

1. Fraude en el campo de la informática.
2. Falsificación en materia informática.
3. Sabotaje informático y daños a datos computarizados o programas informáticos.
4. Acceso no autorizado.
5. Intercepción sin autorización.
6. Reproducción no autorizada de un programa informático protegido.
7. Espionaje informático.
8. Uso no autorizado de una computadora.
9. Tráfico de claves informáticas obtenidas por medio ilícito.

---

[42] **Copyright:** Es el derecho de copia de creaciones de materiales originales sin que medie el plagio o el fraude.

[43] RAMÍREZ BEJERANO, EMILIO y ANA ROSA AGUILERA RODRÍGUEZ. Los delitos informáticos. Tratamiento internacional. Cuba. 2009. p. 10.

10. Distribución de virus o programas delictivos.

La Organización de las Naciones Unidas por su carácter internacional reconoce los distintos tipos de delitos[44] a fin de que los países los tengan en consideración para ser incorporados a sus distintas legislaciones penales correspondientes, los cuales son:

1. Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de los datos de entrada: Este tipo de fraude informático también conocido 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.

- La manipulación de programas: Es muy difícil descubrir y a menudo pasa inadvertido debido a que el delincuente debe tener conocimientos técnicos concretos de 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[45].

- 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 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 computadoras especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

---

[44] Delitos Informáticos reconocidos por Naciones Unidas. Tabla Facultativa. Intranet MININT \ Web Delitos Informáticos \ ismi.htm.

[45] **Caballo de Troya**: Consiste en insertar instrucciones a una computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal, no son capaces de auto propagarse.

- Fraude efectuado por manipulación informática: Aprovecha las repeticiones automáticas de los procesos del cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfiere a otra.

2. Falsificaciones informáticas:

- Como objeto: Cuando se alteran datos de documentos almacenados en forma computarizada.

- 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, puede modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos falsos que producen son de tal calidad que sólo un experto puede diferenciarlo de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados.

- 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 permiten cometer sabotajes informáticos son:

- Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y se proporciona a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
- Gusanos: Se fabrica de forma análoga al virus con miras en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus por que puede regenerarse. En términos médicos podría

decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano subsiguiente se destruirá y puede dar instrucciones a un sistema informático de un banco que transfiera continuamente dinero a una cuenta ilícita.

- Bomba lógica cronológica: Exige conocimientos especializados ya que requiere la programación de destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

- Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. El acceso se efectúa desde un lugar exterior, situado en la red de telecomunicaciones recurriendo a uno de los diversos medios que se mencionan a continuación. 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.

- Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos, algunas jurisdicciones 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 consideramos, que la reproducción no

autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

En Cuba la radicación de esta forma de delito ha sido contradictoria, debido a que las conductas no han sido en su mayoría puras, estando asociadas a elementos de varias conductas de las tipificadas en el Código Penal, posibilitando darle una respuesta jurídica; no obstante a ello han quedando lagunas que no le dan respuestas a todos los elementos de realización de las conductas, no se puede olvidar que muchos de estos delitos tradicionales fueron básicamente creados por los legisladores hace más de un siglo, cuando la informática sólo era un sueño en la mente de unos pocos científicos.

La práctica ha demostrado igualmente que haciendo modificaciones en los delitos tradicionales como se hizo con el Robo con Fuerza, donde se incorporó un inciso relacionado con la aceptación como llave de los mecanismos de apertura magnética, se puede hacer otras modificaciones en otros delitos y de esa forma se le pueda dar una respuesta jurídica acorde con la conducta y la gravedad de los hechos, igualmente se entiende que hay conductas que están fuera de todo contexto legal, en el orden penal, y para ellas hay que establecer nuevas figuras delictivas.

En resumen el uso ilícito de las computadoras puede estar asociado o traer consigo la comisión de delitos tales como: Apropiación Indebida, Malversación, Contrabando, Falsificación de Documentos, Actividad Económica Ilícita, Estafa, Cohecho, entre otros. Pero el problema no radica solo en calificar estas conductas, sino en probar la utilización de la informática para su comisión. En ello puede influir la preparación del personal vinculado a la recolección de la evidencia informática, el procesamiento del delito y las regulaciones acerca de su manipulación.

Capítulo 2: Análisis de la regulación jurídica del Derecho Comparado sobre la criminalidad informática.

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Es cierto que existe un esfuerzo por parte de los países para tratar de evitarlos, aunque no es un criterio unificado de cómo deben ser atacados. Es por eso que se hace imprescindible que se siga trabajando para llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Lo anteriormente señalado ha sido expuesto en diferentes documentos de investigaciones realizadas por la Organización de las Naciones en los cuales se señala que los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Sin embargo la misma ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

1 - Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
2 - Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
3 - Falta de especialización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
4 - Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
5 - Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada, entre ellos, se destacan, Alemania, Francia, Austria, Holanda, España,

Estados Unidos, México, Chile, Venezuela, Guatemala, Colombia, Costa Rica y Argentina.

2.1 – Alemania. Ley de protección de datos.

El 7 de abril de 1970, el Parlamento del estado alemán de Hesse, promulga su normativa de protección de datos *Datenshutz* convirtiéndose en el primer territorio con una norma dirigida a la protección de datos. Después, el 27 de febrero de 1977, el Parlamento Federal de Alemania aprueba la *Datenshutz* Federal. En estos casos se crea un Comisario Federal para la Protección de Datos *(Bundesbeauftragter fur den Datenshutz).*

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica, esta ley reforma el Código Penal[46] para contemplar los siguientes delitos:

Piratería informática: (Artículo 202 a) Establece que la persona que sin autorización se procure para sí o para otros, datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado, será castigado con pena privativa de la libertad hasta tres (3) años o con multa. Considera que los datos son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible. La principal protección jurídica está encaminada a la violación al ámbito de la intimidad personal y al ámbito del secreto personal.

Estafa por computador: (Artículo 263 a) Establece que la persona que con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro por una estructuración

[46] LÓPEZ DÍAZ, CLAUDIA. Traductora. Versión publicada bajo el título Strafgesetzbuch, 32a, edición, Deutscher Taschenbuch Verlag, C. H. Beck, Munich, 1998. Fuente: http://jurcom5.juris.de/bundesrecht/stgb/index.html, actualizado hasta el 30 de agosto de 2002. Código Penal del 15 de mayo de 1871 (RGBl. S. 127), en la versión del 13 de noviembre de 1998 (BGBl. I, 3322), modificada últimamente 34a Ley modificatoria del derecho penal: *§ 129b StGB (34. StrÄndG)* vom 22. August 2002 (BGBl. I, 3390).

incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco (5) años o con multa. Considera que el bien jurídico a proteger es la estafa y la deslealtad.

Alteración de datos: (Artículo 303 a) Considera ilícito que la persona que borre, suprima, inutilice, o cambie antijurídicamente datos, será castigado con pena privativa de la libertad hasta dos (2) años o con multa; incluso la tentativa es punible. En este caso el bien jurídico a proteger es el daño material causado con el hecho delictivo.

Sabotaje informático: (Artículo 303 b) Establece que quien perturbe un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad para cometer un hecho según el artículo 303 a, inciso 1 o 2, destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos será castigado con pena privativa de libertad de hasta cinco (5) años o con multa, considerando punible la tentativa. El bien jurídico que protege es el mismo del párrafo anterior.

2.2 – Francia. Ley No 8819 sobre el fraude informático.

En Francia se crea la Ley 8819[47] del 5 de enero de 1988 sobre el fraude informático la cual contempla dentro de sus apartados.

Acceso fraudulento a un sistema de elaboración de datos: Establece que se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos o resulta la alteración del funcionamiento del mismo.

Sabotaje informático: Se acoge a la persona que intente falsear el funcionamiento de un sistema de tratamiento automático de datos.

[47] Vid. http://www.legifrance.gouv.fr/html/codes_traduits/penal_texte.htm

Destrucción de datos: Establece que se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados: Establece que se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

2.3 – Austria. Ley de reforma del Código Penal.

La Ley de reforma del Código Penal[48] del 22 de diciembre de 1987 contemplan los siguientes delitos:

Destrucción de datos: (Artículo 126) Establece que será sancionable no solo los datos personales sino también los no personales y los programas.

Estafa informática: (Artículo 148) Se sanciona a aquellas personas que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

2.4 – Holanda. Ley de delitos informáticos.

Hasta el día 1 de marzo de 1993 en que entró en vigencia la Ley de delitos informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos las técnicas de Hacking y Phreacking.

Considera que el mero hecho de entrar en una computadora en la cual no se tiene acceso legal se considera delito y puede ser castigado hasta con seis (6) meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro

[48] Vid.http://europa.sim.ucm.es/compludoc/AA?articuloId=119109&donde=castellano&zfr=0.

(4) años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro (4) años en la cárcel, publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal[49].

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis (6) meses a quince (15) años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos (2) años de prisión pero, si se hizo vía remota aumenta a cuatro.

Los virus están considerados de manera especial en la ley si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro (4) años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres (3) años de prisión, considera que la venta de elementos que permitan el Phreaking se castiga con un (1) año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres (3) años.

Recibir datos de transmisiones satelitales es legal, siempre y cuando no haga falta un esfuerzo especial para conseguirlos, la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. La falsificación de tarjetas de crédito de la banca electrónica y el uso para obtener beneficios o como si fueran las originales está penado con hasta seis (6) años de privación de libertad.

[49] Vid. http://www.venelogia.com/ex/tag/Delitos+inform%E1ticos

2.5 – España. Ley Orgánica de protección de datos de carácter personal (LOPD) y el Código Penal.

En España el desarrollo normativo ha estado enmarcado por el Real Decreto 994/1999 de las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal del 11 de junio de 1999. Es un reglamento que desarrolla la Ley Orgánica 5/1992, del 29 de octubre sobre la regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), regula las medidas técnicas y organizativas que deben aplicarse a los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada. (Derogado desde el 19 de abril de 2010)[50]

El Real Decreto 1720/2007 del 21 de diciembre que contempla el desarrollo de la Ley Orgánica de protección de datos, trata de un desarrollo de la Ley Orgánica 15/99 de protección de datos del 13 de diciembre; desarrolla tanto los principios de la ley como las medidas de seguridad a aplicar en los sistemas de información. Se aplica tanto a ficheros en soporte automatizado como en cualquier otro tipo de soportes.

La Ley Orgánica 15/1999 del 13 de diciembre de protección de datos de carácter personal (LOPD), es una ley española que tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad, privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan. La Ley comprende un total de 49 artículos divididos en 7 títulos y finaliza con una serie de disposiciones, dentro de su contenido se encuentran: principios de la protección de los datos, derechos de las personas, ficheros de titularidad pública y privada, movimiento internacional de datos, agencia española de protección de datos e infracciones y sanciones.

[50] Vid. http://delitosinformaticos.com/legislacion/espana.shtml.

Las sanciones tienen una elevada cuantía, siendo España el país de la Unión Europea que tiene las sanciones más altas en materia de protección de datos. Dichas sanciones dependen de la infracción cometida y se dividen en:

- Sanciones leves, establece una cuantía a pagar de 601,01 a 60 101.21 € (Euros).
- Sanciones graves, establece una cuantía a pagar de 60 101,21 a 300 506,05 € (Euros).
- Sanciones muy graves, establece una cuantía a pagar de 300 506,05 a 601 012,10 € (Euros).

En esta ley los datos personales se clasifican en función de su mayor o menor grado de sensibilidad, siendo los requisitos legales y las medidas de seguridad informáticas más estrictas en función de su grado de sensibilidad, y es obligatorio por otro lado en todo caso la declaración de los ficheros de protección a la "Agencia Española de protección de datos".

En España la seguridad informática cuenta con un cuerpo legislativo que regula los aspectos de la sociedad de información, entre los que se encuentran:

- Ley Orgánica 15/1999, del 13 de diciembre de protección de datos de carácter personal.
- Ley 34/2002, del 11 de junio de servicios de la sociedad de la información y comercio electrónico.

- Real Decreto Ley 1/1996 del 12 de abril por el que se aprueba el texto refundido de la Ley de propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia con las modificaciones realizadas por la Ley 1/2000 del 7 de enero de enjuiciamiento civil.
- Real Decreto Ley 14/1999 del 17 de septiembre sobre firma electrónica.
- Ley 59 del 19 de diciembre de 2003 de firma electrónica, promulgada para reforzar el marco jurídico existente e incorporando a su texto algunas novedades respecto al Real Decreto Ley 14/1999 como respuesta a la necesidad de conferir seguridad a las comunicaciones por internet y que tiene como objeto regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

El Código Penal (Ley Orgánica 10/1995) contempla artículos específicos referentes a los delitos informáticos dentro de los que se puede enmarcar:

Descubrimiento y revelación de secretos: (Artículo 197) El que vulnere la intimidad sin el consentimiento, se apodere de mensajes de correo electrónico, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción de sonidos o imágenes; será castigado con pena de prisión de uno (1) a cuatro (4) años o multa de doce (12) a veinticuatro (24) meses. Prevé la protección a los datos reservados de carácter personal o familiar donde se hallen registrados ficheros o soportes informáticos y reprime también si se realiza por las personas encargadas, responsables, autoridad o funcionario público de los ficheros, soportes informáticos, electrónicos o telemáticos; estableciendo una sanción agravada de dos (2) a cinco (5) años de prisión. La objetividad jurídica a proteger en este caso son los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

De los robos: (Artículo 238) Establece que se consideran reos de delitos de robo con fuerza los que hagan utilización de sistemas específicos de alarma o conserva el uso de llaves falsas considerando así a las tarjetas magnéticas o perforadas, los mandos o instrumentos de apertura a distancia, previendo una sanción de prisión de uno (1) a tres (3) años. Se protege jurídicamente a los delitos contra el patrimonio y el orden socioeconómico.

De las estafas: (Artículo 248) Contempla que se considera reo de estafa al que con ánimo de lucro y valiéndose de una manipulación informática o artificio semejante consiga la transferencia de cualquier activo patrimonial, siendo sancionable de seis (6) meses a cuatro (4) años de prisión. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador y los medios empleados.

De los daños: (Artículo 264) Considera que será castigado 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

siendo castigado con pena de prisión de uno (1) a tres (3) años o multa de doce (12) a veinticuatro (24) meses.

Delitos relativos a la propiedad intelectual: (Artículo 270) Establece que será castigada la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador, siendo sancionable de seis (6) meses a dos (2) años de prisión o multa de seis (6) a veinticuatro (24) meses.

Delitos relativos al mercado y a los consumidores: (Artículo 270) Propone que la persona que para descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos, escritos electrónicos y soportes informáticos, será objeto de sanción penal de seis (6) meses a dos (2) años de prisión o multa de seis (6) a veinticuatro (24) meses.

De las falsificaciones: (Artículo 400) Considera un hecho punible la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos específicamente destinados a la comisión de delitos de falsificación.

Delitos cometidos por funcionarios públicos: (Artículo 536) La persona que intercepte las telecomunicaciones o utilizare artificios técnicos de escucha, transmisión, grabación o reproducción de sonido, imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales será objeto de sanción especial consistente en inhabilitación para el empleo o cargo público de dos (2) a seis (6) años; si divulga o revela la información obtenida se impondrán las penas de inhabilitación especial en su mitad superior o multa de seis (6) a dieciocho (18) meses. La objetividad jurídica a proteger en ese caso son los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad.

El Código Penal considera como una pena grave la prisión superior de tres (3) años y la multa de más de dos (2) meses (Artículo 33), respecto a esta última consigna que la razón a pagar se realizará por una cuota diaria.

2.6 – Estados Unidos.

Los Estados Unidos se caracterizan por tener una legislación variada en cuanto a la prevención y sanción de los hechos cometidos que generan la criminalidad informática, pudiendo mencionar la Ley Federal de protección de sistemas (1985), la Ley Federal sobre fraude mediante transmisiones por cable, el Acta de privacidad en las comunicaciones electrónicas (1986), el Acta de seguridad informática para el desarrollo económico y la educación, el Acta Federal contra el abuso computacional (1994, 18 U.S.C Sec. 1030) y el Acta de espionaje económico (1996). Todo lo anterior se encuentra a nivel federal, por lo que ninguna duda debe caber acerca de la existencia de una abundante legislación dentro de cada uno de los más de cincuenta estados[51].

En 1994 se adoptó el Acta Federal de abuso computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986, donde se contempla la regulación de los virus (computer contaminant), conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Considera que modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es apreciado como delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país tras un año largo de deliberaciones establece el Acta de firmas electrónicas en el comercio global y nacional, respondiendo a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante internet entre empresas o entre empresas y consumidores.

[51] Vid. http://lawiuris.wordpress.com/2009/06/02/el-delito-informatico/

2.7 – México. Ley Federal de protección de datos personales y el Código Penal.

La Ley Federal de protección de datos personales[52] tiene por objeto asegurar que el trato de los datos personales se realice respecto a las garantías de las personas físicas y jurídicas proponiendo que en ningún caso se podrán afectar los registros y fuentes periodísticas.

Considera que son los datos de carácter personal los que figuran en archivos, registros, bancos o bases de datos de personas físicas o jurídicas, públicas o privadas, y a todo uso posterior, incluso no automatizados, y de carácter personal registrados en soporte físico susceptible de tratamiento automatizado. La sensibilidad de los mismos es relativo a condenas y sanciones penales, sólo se pueden tratar automatizadamente para su acceso al público o a institución no competente con el permiso previo del interesado y siempre que el responsable del archivo, registro, base o banco de datos garantice a satisfacción del Instituto Federal de Protección de Datos Personales la disociación de los datos.

Expresa que el interesado o responsable de los registros tiene derecho a que se le informe de manera expresa la existencia y colecta de un archivo, registro, base o banco de datos de carácter personal, de las consecuencias de la obtención de los datos o de la negativa de suministrarlos; la posibilidad de ejercitar los derechos de acceso, inclusión, complementación, rectificación, suspensión, reserva y cancelación. Cuando se colecta de fuentes de información de acceso público, para el ejercicio de las funciones propias de entidades y organismos públicos en el ámbito de su competencia no requiere de consentimiento.

La mencionada ley establece la prohibición de proporcionar datos personales, formación de archivos, registros, bases o bancos que revelen datos sensibles, estos solo se pueden ceder a personas con interés legítimo con el previo consentimiento del interesado. La transferencia de datos personales con Estados u Organismos

[52] Vid. http://www.tuabogadodefensor.com/01ecd193e810f1e01/Penal/index_dinform.htm

Internacionales que no proporcionen niveles de seguridad y protección. Los datos de carácter público solo se pueden crear, modificar o extinguir por medio de disposiciones de carácter general.

Las infracciones se clasifican en leves y graves. Considera como leve la referente a omitir la inclusión, complementación, rectificación, actualización, reserva, suspensión o cancelación de oficio de los datos personales que obren en archivos, registros, bases o bancos de datos; y graves la colecta de datos de carácter personal sin titularidad pública sin la previa autorización de la normativa aplicable, impedir u obstaculizar el ejercicio del derecho de acceso y violentar el secreto empresarial. Prevé como sanciones el apercibimiento, suspensión de operaciones, multa de uno a cien días de salario mínimo, clausura o cancelación del archivo, registro o banco de datos.

El Código Penal de México dedica el Título Noveno a la revelación de secretos y acceso ilícito a sistemas y equipos de informática dentro de ellos se puede mencionar:

Revelación de secretos: (Artículo 210) Constituido por el que sin justa causa, con perjuicio de alguien y sin consentimiento de que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto o información o imágenes obtenidas en una intervención de comunicación y será objeto de sanción de treinta (30) a doscientas (200) jornadas de trabajo a favor de la comunidad o de uno (1) a cinco (5) años de multa de cincuenta ($ 50) a quinientos ($ 500) pesos.

Acceso ilícito a sistemas y equipos de informática: (Artículo 211) Se considera un hecho punible el que sin autorización o siendo autorizado indebidamente, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad ya sea del Estado o de instituciones del sistema financiero; siendo objeto de sanción de seis (6) meses a dos (2) años de prisión o de cien a trescientos días de multa, contempla una sanción agravada de uno (1) a cuatro (4) años de privación de libertad y de doscientos a seiscientos días de multa.

2.8 – Chile. Ley No 19223 sobre delitos informáticos.

En Chile se introduce en el ordenamiento jurídico diversas figuras penales relacionadas con los delitos informáticos, mediante la promulgación de la Ley No 19223 sobre delitos informáticos[53], del 28 de mayo de 1993 publicada en el Diario Oficial No 34.584, la cual contempla:

Sabotaje informático a los sistemas de tratamiento de información: Se considera como toda conducta típica, antijurídica y culpable al que maliciosamente atente contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en el, los destruya, impida, obstaculice o modifique; sufriendo así una pena de presidio menor en su grado medio o máximo. Sus direcciones de protección son las siguientes:

Acciones contra el sistema y tratamiento de la información: Comprende la destrucción o inutilización de un sistema automatizado de tratamiento de la información.

Acciones contra el funcionamiento de un sistema de tratamiento de la información: El objetivo fundamental es impedir el funcionamiento del sistema, su desempeño, manejo, también modificar el sistema de tratamiento de la información o de sus partes componentes.

Conductas que afecten los datos conferidos en un sistema de tratamiento de la información: El objetivo se desarrolla a través de tres tipos de conductas: Alterar, dañar o destruir los datos contenidos en un sistema de tratamiento de información.

Espionaje informático: Su finalidad va encaminada a la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información; previendo al que con ánimo de apoderarse, usar o conocer indebidamente, intente, interfiera o acceda; sancionándolo con presidio menor en su grado mínimo a medio. Se ha agrupado esta en las siguientes categorías:

---

[53] HUERTA MIRANDA, MARCELO. Abogado. Mag. Iur Unds Soziologie fur Juristen, U. Salzburg. Presidente de la Asociación de Derecho e Informática de Chile. Revista Electrónica REDI. Chile. 2008. p. 15.

Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información: Dentro de las conductas típicas se encuentra la interferencia, intercepción y acceso indebido de la información contenida en un sistema de tratamiento de información, burlando todas las medidas de seguridad y resguardo de programas en su entrada.

Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de información: Contempla la revelación en cuanto a la difusión que se realice maliciosamente, tratando así de proteger la fidelidad en la custodia de informaciones, evitándose la vulneración de la obligación de debida reserva que pesa no solo respecto de la persona encargada de la administración de la información y los datos.

2.9 – Venezuela. Ley Especial contra delitos informáticos.

En Venezuela se ofrece un tratamiento penal a las conductas que atentan contra la seguridad informática mediante la Ley Especial contra los delitos informáticos[54] de fecha 6 de septiembre de 2001, tiene como objeto la protección integral de los sistemas que utilizan 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. La mencionada ley ofrece los conceptos de tecnología de la información, sistema, data, información, documento, computador, hardware, firmware, software, programa, seguridad, virus, entre otros. Clasifica los delitos en:

1. Delitos contra los sistemas que utilizan tecnologías de información.

Acceso indebido: (Artículo 6) 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 (1) a cinco (5) años y multa de diez (10) a cincuenta (50) unidades tributarias.

[54] Vid. http://www.iuspenalismo.com.ar/doctrina/informaticos.htm

Sabotaje o daño a sistemas: (Artículo 7) 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, así como si se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas; la pena será de cinco (5) a diez (10) años de prisión y multa de quinientas (500) a mil (1 000) unidades tributarias, si los efectos indicados en el presente artículo se realizaran mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Posesión de equipos o prestación de servicios de sabotaje: (Artículo 10) 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 o dispositivos; o el que ofrezca o preste servicios destinados a cumplir los mismos fines será penado con prisión de tres (3) a seis (6) años y multa de trescientas (300) a seiscientas (600) unidades tributarias.

Espionaje informático: (Artículo 11) 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 (4) a ocho (8) años y multa de cuatrocientas (400) a ochocientas (800) 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.

Falsificación de documentos: (Artículo 12) El que a través de cualquier medio, 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 (3) a seis (6) años y multa de trescientas (300) a seiscientas (600) unidades tributarias. Cuando el agente hubiera 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.

2. Delitos contra la propiedad.

Hurto: (Artículo 13) El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema 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 (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Fraude: (Artículo 14) 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 (3) a siete (7) años y multa de trescientas (300) a setecientas (700) unidades tributarias**.**

Obtención indebida de bienes y servicios: (Artículo 15) 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 (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Manejo fraudulento de tarjetas inteligentes o instrumentos análogos: (Artículo 16) 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, 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 (5) a diez (10) años y multa de

quinientas (500) a mil (1 000) 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.

Provisión indebida de bienes o servicios: (Artículo 18) El que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, han sido falsificados, alterados, se encuentran vencidos o revocados o han sido indebidamente obtenidos o retenidos, provea a quien los presente, de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Posesión de equipo para falsificaciones: (Artículo 19) 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 (3) a seis (6) años y multa de trescientas (300) a seiscientas (600) unidades tributarias.

3. Delitos contra la privacidad de las personas y de las comunicaciones.

Violación de la privacidad de la data o información de carácter personal. (Artículo 20) El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o informaciones personales de otros 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 (2) a seis (6) 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.

Violación de la privacidad de las comunicaciones: (Artículo 21) 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 ajenos, incurrirá en la pena de dos (2) a seis (6) años de prisión y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Revelación indebida de data o información de carácter personal: (Artículo 22) 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 los medios informáticos, será sancionado con prisión de dos (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias, si hubiera realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Difusión o exhibición de material pornográfico: (Artículo 23) El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda libremente, de modo que pueda ser accedido por niños o adolescentes, material pornográfico o reservado a personas adultas, será sancionado con prisión de dos (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

Exhibición pornográfica de niños o adolescentes: (Artículo 24) El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro (4) a ocho (8) años y multa de cuatrocientas (400) a ochocientas (800) unidades tributarias.

4. De los delitos contra el orden económico.

Apropiación de propiedad intelectual: (Artículo 25) 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 (1) a cinco (5) años y multa de cien (100) a quinientas (500) unidades tributarias.

Oferta engañosa: (Artículo 26) 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 (1) a cinco (5) años y multa de cien (100) a quinientas (500) unidades tributarias, sin perjuicio de la comisión de un delito más grave.

En un cuerpo legal independiente, Decreto Ley sobre mensajes de datos y firmas electrónicas, de 2001, regula la eficacia y el valor jurídico de la firma electrónica, el mensaje de datos y toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, además regula todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos; ofreciéndoles una tutela administrativa.

2.10 - Guatemala. El delito informático en el Código Penal.

El Código Penal[55] para darle tratamiento a la criminalidad informática contempla dentro de los Delitos contra el patrimonio el Capítulo VII Sobre los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, dándole una especial protección al uso y cuidado de los datos para lo cual establece las siguientes figuras delictivas:

Destrucción de registros informáticos: (Artículo 274 a) Contempla que el que destruya, borre o de cualquier modo inutilice registros informáticos será objeto de sanción con prisión de seis (6) meses a cuatro (4) años, y multa de doscientos (200) a dos mil (2 000) quetzales.

Alteración de programas: (Artículo 274 b) Será objeto de sanción la persona que altere, borre o de cualquier modo inutilice las instrucciones o programas que utilizan las computadoras.

Reproducción de instrucciones o programas de computación: (Artículo 274 c) Contempla que la persona que sin autorización del autor, copie o de cualquier modo reproduzca las instrucciones o programas de computación será reprimido con sanción

[55] Vid. Código Penal y Exposición de Motivos. 1ª ed. Guatemala. Ediciones Especiales. Edición de Colección Temas Jurídicos, s/f.e. p. 332.

penal de prisión de seis (6) meses a cuatro (4) años y multa de quinientos (500) a dos mil quinientos (2 500) quetzales.

Registros prohibidos: (Artículo 274 d) Establece que la persona que cree un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas será objeto de sanción de prisión de seis (6) meses a cuatro (4) años y multa de doscientos (200) a mil (1 000) quetzales.

Manipulación de información: (Artículo 274 e) Considera que la persona que utilice registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica será reprimida con sanción penal de prisión de uno (1) a cinco (5) años y multa de quinientos (500) a tres mil (3 000) quetzales.

Uso de información: (Artículo 274 f) Establece que la persona que sin autorización, utilice los registros informáticos de otro, o ingrese por cualquier medio a su banco de datos o archivos electrónicos será objeto de sanción de prisión de seis (6) meses a dos (2) años, y multa de doscientos (200) a mil (1 000) quetzales.

Programas destructivos: (Artículo 274 g) Contempla a la persona que distribuya o ponga en circulación programas o instrucciones destructivas, que pueda causar perjuicio a los registros, programas o equipos de computación se le impondrá la sanción de prisión de seis (6) meses a cuatro (4) años, y multa de doscientos (200) a mil (1 000) quetzales.

2.11 - Colombia. Ley No 1273 sobre delitos informáticos.

En Colombia se encuentra vigente la Ley No 1273 sobre los delitos informáticos[56], promulgada el 5 de enero de 2009, su objetivo principal es elevar a bien jurídico

[56] Vid. http://www.lavozdelsandinismo.com/ciencia-tecnica/2010-062/adiestraran-a-fiscales-sobre-delitos-informaticos/

tutelado la información y los datos, la presente norma está compuesta por dos capítulos con las siguientes figuras delictivas:

Capítulo I: Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicaciones, intercepción de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios Web para capturar datos y circunstancias de agravación punitiva.

Capítulo II: Hurtos por medios informáticos y semejantes transferencia no consentida de activos.

2.12 - Costa Rica. Ley No 8148 reforma del Código Penal.

Se encuentra vigente la Ley No 8148[57] la cual decreta la adición de los artículos (196 Bis, 217 Bis y 229 Bis) al Código Penal, promulgada el 24 de octubre de 2001; para reprimir y sancionar los siguientes delitos informáticos:

Violación de comunicaciones electrónicas: (Artículo 196 Bis) Considera que la persona que se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en soportes electrónicos, informáticos, magnéticos y telemáticos sin el debido consentimiento para descubrir los secretos o vulnerar la intimidad de otros será reprimida con pena de prisión de seis (6) meses a dos (2) años, la pena será de uno (1) a tres (3) años de prisión si las acciones descritas son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

Fraude informático: (Artículo 217 Bis) Contempla que 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 sistemas se impondrá pena de prisión de uno (1) a diez (10) años.

[57] Vid. http://www.legifrance.gouv.fr/html/codes_traduits/penal_textE.htm

Alteración de datos y sabotaje informático: (Artículo 229 Bis) Establece que la persona que por cualquier medio acceda, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora se impondrá pena de prisión de uno (1) a cuatro (4) años. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa del cómputo una base de datos o un sistema informático, la pena será de tres (3) a seis (6) 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 (8) años.

2.13 - Argentina. Ley No 26.388 reforma del Código Penal.

En Argentina es sancionada el 4 de junio de 2008 y promulgada de hecho el 24 de junio de 2008 por el Senado y la Cámara de Diputados de la nación reunidos en el Congreso, la Ley No 26.388 que reforma el Código Penal[58] y la sanciona con fuerza de Ley.

La presente norma incorpora como últimos párrafos del artículo 77 del Código Penal, el término "documento" estableciendo que comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" que comprenden la firma digital, la creación de una firma digital o firmar digitalmente, "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Acceso indebido: (Articulo 4 que sustituye el artículo 153 del Código Penal) Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. La objetividad jurídica a proteger es la "Violación de los secretos y de la privacidad".

[58] Vid. http://www.segu-info.com.ar/delitos/delitos.htm

Se incorpora como artículo 153 bis del Código Penal estableciendo que será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Intercepción de comunicaciones: En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunica a otro o publica el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo comete un funcionario público que abusa de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Publicación y revelación de información: (Artículo 155) Será reprimido con multa de mil quinientos ($ 1.500) a cien mil ($ 100.000) pesos, el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los haga publicar indebidamente, si el hecho causa o pueda causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Fraude: (Artículo 9 incorporado como inciso 16 del artículo 173 del Código Penal) Será objeto de sanción penal la persona que defraude a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Destrucción: (Artículo 10 incorporado como segundo párrafo del artículo 183 del Código Penal) Establece que en la misma pena incurrirá el que altere, destruya o inutilice datos, documentos, programas o sistemas informáticos; o venda, distribuya,

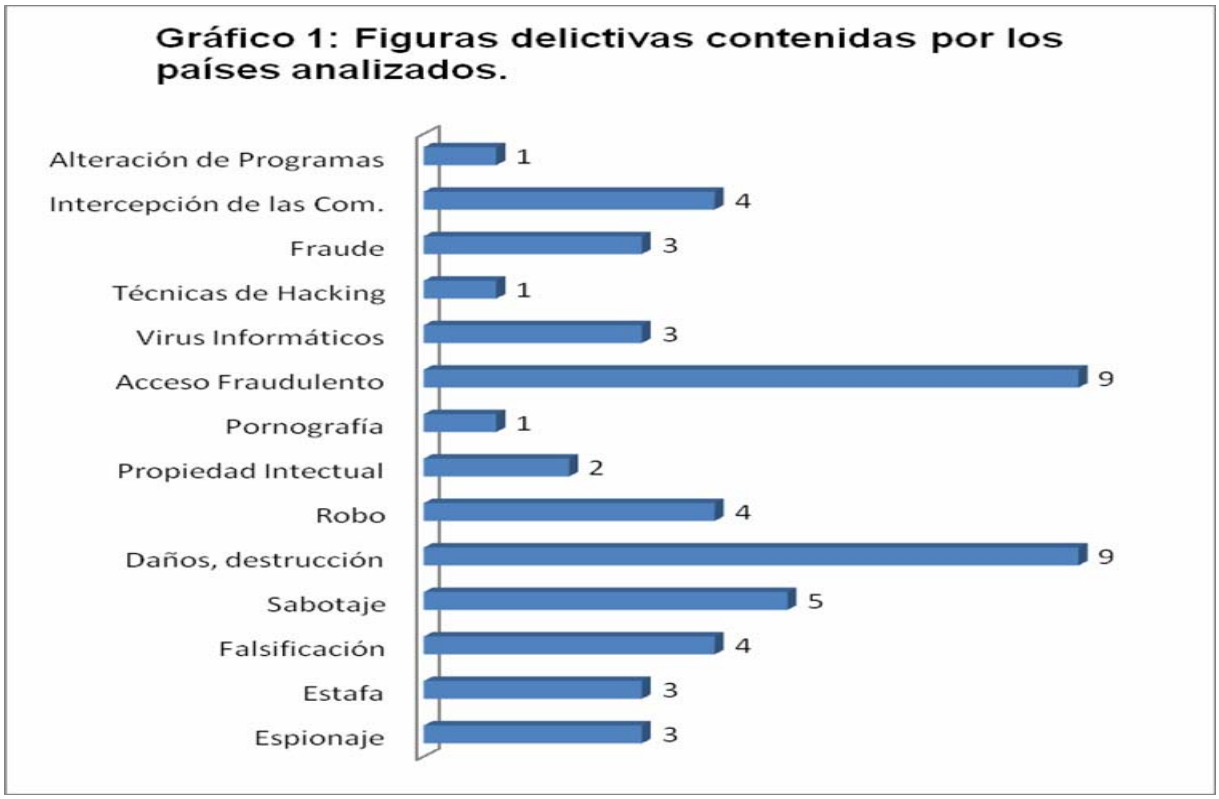
haga circular o introduzca en un sistema informático, cualquier programa destinado a causar daños.

El artículo 11 que sustituye al artículo 184 del Código Penal establece como circunstancia adecuativa que la pena será de tres (3) meses a cuatro (4) años de prisión si el programa se ejecuta en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

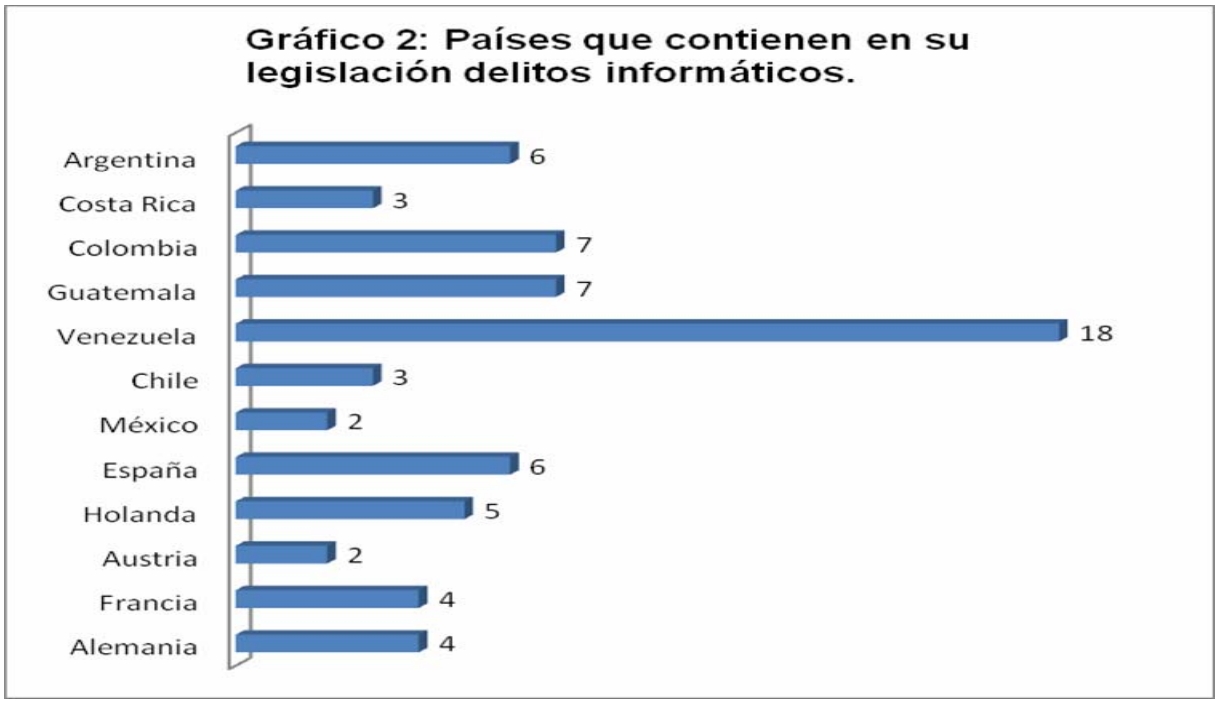
Interrupción de comunicaciones: (Artículo 12 que sustituye el artículo 197 del Código Penal) Considera que será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpa o entorpezca la comunicación telegráfica, telefónica o de otra naturaleza o resista violentamente el restablecimiento de la comunicación interrumpida.

2.14 – Evaluación de la legislación comparada.

Teniendo en cuenta el análisis realizado a la legislación comparada la que ha pretendido encuadrar estas figuras delictivas ajustándose a su contexto nacional, se ha podido constatar que existen 8 figuras delictivas relacionadas con delitos tradicionales, tales como: espionaje, estafa, falsificación, sabotaje, daños o destrucción, robo, abuso de la propiedad intelectual y pornografía, y 6 figuras de nueva creación, tales como: acceso fraudulento o revelación de datos, virus informáticos, técnicas de hacking, violación o intercepción de las comunicaciones y alteración de programas informáticos; dentro de los delitos que más presencia ha tenido en las legislaciones se encuentra el de daños o destrucción (9) y el de acceso fraudulento o revelación de datos (9). Así lo muestra el siguiente gráfico donde se analiza el delito y la cantidad de países donde ha sido establecido.



Dentro de los países que mas delitos calificados presentan en su legislación se encuentra Venezuela la que posee una legislación propia para reprimir estas conductas en la cual tiene contenida 18 figuras delictivas que abarcan una amplia gama, protegiendo objetividades jurídicas tales como el delito contra los sistemas que utilizan tecnologías, contra la propiedad, contra la privacidad de las personas y de las comunicaciones y contra el orden económico. También se encuentra Chile donde aborda específicamente el sabotaje y el espionaje y Colombia que posee 7 calificaciones dentro de las que se pueden mencionar: acceso abusivo, uso de software malicioso, hurto de medios informáticos, etc. Así lo muestra el siguiente gráfico donde se plasman los países que han contenido en su legislación figuras delictivas.

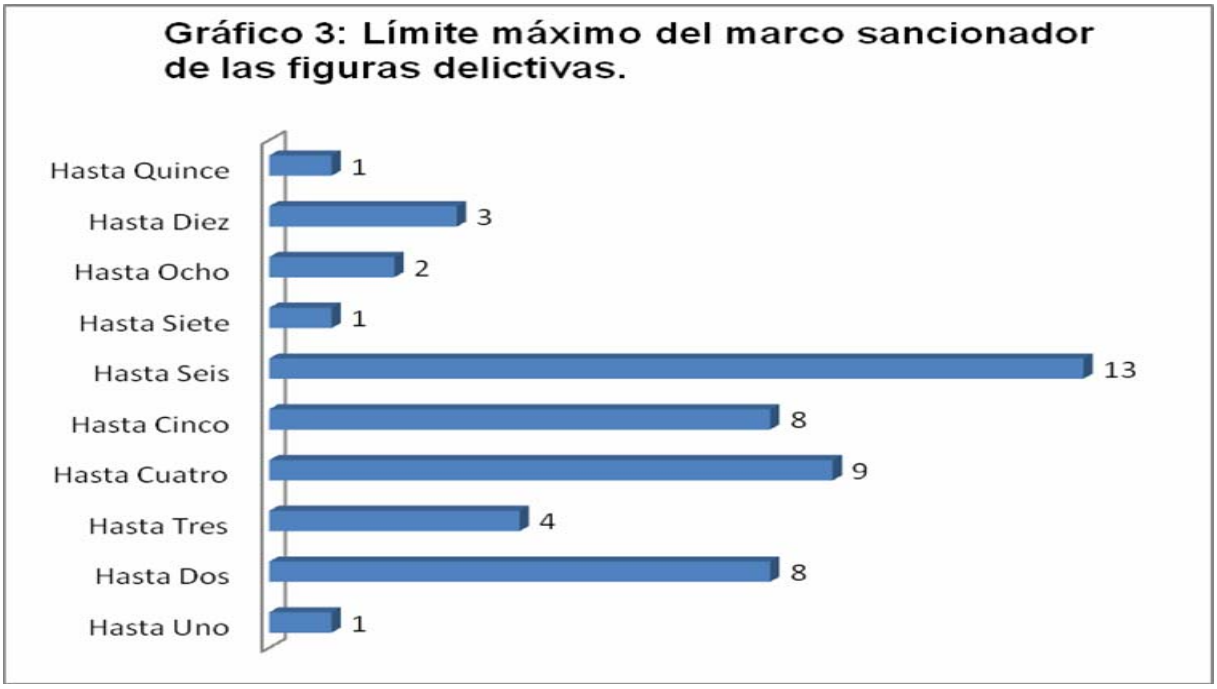


En cuanto a los países de la región de América Latina que poseen delitos específicos dentro de sus Códigos Penales se encuentran México con dos calificaciones (revelación de datos y acceso ilícito), Guatemala con 7 calificaciones (destrucción de registros informáticos, alteración de programas, reproducción de programas, etc...) siendo el país que más figuras presenta en su legislación penal, Costa Rica con 3 calificaciones (violación de la correspondencia, fraude informático, alteración de datos y sabotaje).

Dentro de los países que ha dado especial protección al cuidado y uso de los datos es encuentra España y Alemania con una ley específica que protege a las informaciones dando una amplia calificación y clasificaciones a los mismos.

En cuanto a la forma de reprimir dichas manifestaciones se ha comprobado que las sanciones varían según el tipo de delito y la magnitud del mismo, desde un (1) año hasta (15) años, siendo la sanción más severa a imponer la de daño a la información en Holanda con privación de libertad de hasta quince (15) años, la sanción que mas se impone es la de hasta seis (6) años de prisión siendo Venezuela, Guatemala, y España los que más la utilizan en delitos tales como: agravante de sabotaje, obtención indebida de bienes y servicios, falsificación de documentos, tarjetas, revelación indebida de datos, violación de la privacidad de las comunicaciones, etc. España uno de los países

Europeos que más fuerte tiene las penas dentro de las que cabe mencionar prisión de uno (1) a cuatro (4) años, con su agravante de dos (2) a cinco (5) años en el delito de descubrimiento y revelación de secretos, y una media que varia de uno (1) a cuatro (4) años en seis figuras delictivas, también establece una cuantía a pagar que asciende hasta los seis cientos mil euros según el tipo de sanción. A continuación se muestra un gráfico que ilustra el límite máximo de años a reprimir según las tipicidades.



En el caso de la sanción de hasta un (1) año de prisión se encuentra Argentina con el delito de acceso indebido, hasta dos (2) años se encuentran Alemania, España, México, Costa Rica y Argentina en delitos como: alteración de datos, acceso ilícito, uso de información; hasta tres (3) años se hallan España, Alemania y Holanda con los delitos de: daño, piratería, robo, hasta cuatro (4) años se encuentran Guatemala, España, Costa Rica, Argentina con figuras delictivas tales como: destrucción de información, reproducción de instrucciones, acceso ilícito, virus informático, estafa sabotaje; hasta cinco (5) años están Alemania, México, Venezuela y España con delitos tales como: estafa, sabotaje, agravante del descubrimiento y revelación de secretos, manipulación informática, hasta seis (6) años se hallan Guatemala, Venezuela y España con delitos tales como: agravante de sabotaje, obtención indebida de bienes y servicios, falsificación de documentos, posesión de equipos para falsificaciones, hurto, revelación

indebida de datos y pornografía, hasta siete (7), ocho (8) y diez (10) años se halla Venezuela y Costa Rica con los delitos de: fraude informático, espionaje, pornografía de niños, manejo fraudulento de tarjetas inteligentes y sabotaje, hasta quince (15) años se encuentra Holanda con el delito de daño de información. En la medida que la sanción va aumentando pasado los seis (6) años de privación de libertad disminuyen los delitos plasmados.

Dentro de los países de la región se encuentra Venezuela como el país que más fuerte presenta las sanciones, en las que el límite máximo del marco sancionador se encuentra entre los cinco (5) y diez (10) años de prisión, Costa Rica con sanción de uno (1) a diez (10) años en el caso del delitos de fraude informático. Todo ello a corroborado que el delito que más fuerte se sanciona el que guarda relación con la protección de datos existiendo similitud con nuestro país que aboga que son los datos los que más rápidos se devalúan puesto que son accedidos por mas usuarios que el resto de las aplicaciones.

Capítulo 3: Propuesta de modificaciones al tratamiento legal de la criminalidad informática en Cuba.

La amplia diversidad de uso y funciones que ofrecen los sistemas informáticos logran potencializar las posibilidades de las distintas figuras delictivas contenidas en el Código Penal vigente, y aun dar sustento a la aparición de nuevas ilicitudes que sólo se conciben con el uso de las Tecnologías de la Informática y las Comunicaciones. Podemos decir entonces que con el desarrollo de la informática, hace aparición un nuevo tipo de delincuencia, sofisticada, de calidad superior, capaz en sí misma de aparejar nuevos problemas al derecho penal y a la administración de justicia; siendo así nuestra legislación actualmente lo que ha realizado es tipificar estas conductas mediante los delitos vigentes los cuales han ido en ascenso. (Ver Anexo 2).

3.1 – Análisis de las figuras delictivas establecidas en el Código Penal vigente que guardan relación con las TIC y la Resolución 127 de 2007 del Ministerio de la Informática y las Comunicaciones.

3.1.1 - Delitos contra la seguridad del Estado.

Las agresiones a nuestro país han estado matizadas por diversidad de actos ilícitos, todos proyectados, organizados y financiados desde el exterior, dirigidos fundamentalmente a la realización de acciones militares, políticas, económicas e ideológicas para estrangular al país, propiciar y estimular los focos de oposición, el aislamiento en el plano internacional, lograr por todas las vías la eliminación de los principales dirigentes de la revolución, incentivar a los grupos de la oposición interna, los que interactúan directamente con el Gobierno de Estados Unidos y con algunas representaciones extranjeras e incluso tratar de coincidir la disidencia con las opciones legislativas de las elecciones en Cuba, tratando de incorporar elementos contrarrevolucionarios en la estructura estatal y legislativa del país.

El Estado cubano considera una insuficiencia reducir el concepto de seguridad a lo estrictamente militar, porque se ha de tener en cuenta su relación con lo económico,

político y social, pues las inestabilidades en estos campos afectan tanto la seguridad nacional como la regional.[59]

Conforme a su objetividad jurídica, los delitos contra la seguridad del Estado, se insertan entre aquellos delitos que agreden o ponen en peligro los bienes jurídicos de la colectividad, diferenciándose así de los bienes jurídicos que protegen al individuo o los llamados personalísimos[60]. De esta forma en estos delitos se protege la integridad estatal y la soberanía, la forma de gobierno y su desarrollo, la garantía de los ciudadanos de la nación y las relaciones con otros Estados.

Espionaje.

El Espionaje es la obtención secreta de información que la fuente informativa no desea revelar. El término se puede emplear en referencia a los ámbitos militares, económicos o políticos y en general se relaciona con la política exterior y la defensa de los Estados[61]. Emplea micrófonos, aparatos fotográficos, censores, detectores, satélites artificiales, el empleo de la informática y otras técnicas, para descubrir y conseguir información secreta.

Esta conducta delictiva está caracterizada por la relación del sujeto con un servicio de información de un Estado extranjero y justamente la penalidad prevista para el apartado primero del artículo 97 viene dada por participar, colaborar o mantener relaciones con éste, con el propósito de menoscabar o dañar la seguridad del Estado cubano. Es necesario el vínculo entre el sujeto activo y la agencia de información del Estado extranjero para configurar el tipo básico.

En lo que respecta al apartado segundo, se sanciona con igual sanción cuando los datos proporcionados al Estado extranjero tienen el carácter de secreto. Datos,

---

[59] Defensa Nacional. Unidad, Independencia y Soberanía. Colectivo de Autores. Colegio de Defensa Nacional. Ediciones Verde Olivo. Cuba. 1997. p. 39.

[60] VEGA VEGA, JUAN. Los Delitos. Ediciones Estudios. Instituto Cubano del Libro. Cuba. La Habana. 1968. p. 2. Refiriéndose a los delitos contra la seguridad del Estado expresó: "En realidad todos los bienes jurídicamente protegidos interesan a la colectividad y su agresión o puesta en peligro constituye una agresión o puesta en peligro a la colectividad, hay bienes cuya protección interesa más profundamente a todos los miembros de una nación, a todos los ciudadanos de un país."

[61] Diccionario Encarta "Enciclopedia Microsoft". Encarta 2009.

informes o noticias secretas deben considerarse, aquellas respecto de las cuales el vínculo del secreto deriva de manera directa de la naturaleza de los hechos o de las cosas a las cuales ésta se refiere, y que por tanto son conocidas o conocibles por un restringido y determinado número de personas calificadas. Secreto también es aquello que esta destinado a permanecer oculto al conocimiento de otros y conocido sólo por unos pocos o por una sola persona.

El Espionaje previsto en el apartado 3 es conocido como Inteligencia Visual, prohibido por la Ley de Secreto Estatal y por las disposiciones internas de los lugares a que se hace mención[62].

Propaganda enemiga.

Se establece que la propaganda es algo que se difunde y es del conocimiento de varias personas. No es más que difundir entre un grupo de personas. Por esta razón salvo que se exteriorice la conducta por medio de la propaganda escrita, las frases de contenido incitante, tienen que estar dirigidas a la objetividad jurídica que se tutela en esta conducta: el orden social, la solidaridad internacional y el Estado Socialista. Los gritos subversivos, deben tener cierta eficacia inductiva para que tipifique la conducta delictuosa, demostrable con el resultado acaecido y el ánimo del agente. En este supuesto de que la incitación sea oral, no cabrán las formas imperfectas de ejecución.

La confección de la propaganda puede ser intelectual según lo regula el artículo 103.b al dar la idea o material. Siempre que sean publicaciones también habrá clandestinidad de impreso, conexidad sustantiva que de plantearse difiere conforme a la naturaleza jurídica del artículo 210 en tanto la clandestinidad de impreso tiene una finalidad de índole material y el delito protege la anarquía de impresión.

---

[62] Ley No 62. Código Penal. Cuba. Artículo 97. 3: El que, sin la debida autorización, practique reconocimientos, tome fotografías, procure u obtenga informes o levante, confeccione o tenga en su poder planos, croquis o vistas de campamentos, emplazamientos, zonas o unidades militares, obras o medios de defensa, ferrocarriles, barcos o aeronaves de guerra, establecimientos marítimos o militares, caminos u otras instalaciones militares o cualquier otro documento o información concerniente a la seguridad del Estado, incurre en sanción de privación de libertad de cinco a veinte años.

Sabotaje.

Este artículo 104.1 es de los más complejos por su construcción y contiene el dolo específico con el propósito del agente de una parte puede ser provocar la interrupción de medios, recursos, edificaciones, instalaciones, etc., y el dolo eventual o por representación está presente porque el legislador castiga la conducta aún y cuando el agente sin proponérselo realiza los actos saboteadores a sabiendas de que se afecta y perjudica la economía nacional[63], la salud pública, los servicios sociales y otros intereses de la nación. De ahí que en este delito es determinante a los efectos de su comisión, el propósito limitado del agente, en tanto no tiene que tener la intención de afectar la Seguridad del Estado, basta con que se produzca. Por lo tanto el delito excluye la culpa y admite las formas imperfectas de ejecución.

3.1.2 - Delitos contra la Fé Pública.

Falsificación de moneda.

Los comportamientos que resultan penados en el referido artículo 248 Código Penal son: *fabricar, alterar, introducir y tener*. Sobre el particular se ha dicho[64] que las conductas previstas pueden diferenciarse entre las que constituyen formas "de ipso" o de primer grado como es la fabricación de la moneda falsa y la alteración de la moneda legítima, y las formas "ex post" o de segundo grado; así la introducción en el país y la tenencia de moneda falsa, puesto que sólo las primeras constituyen la conducta falsaria

[63] Ley No 62. Código Penal. Cuba. Artículo 104. 1. Incurre en sanción de privación de libertad de dos a diez años el que, con el propósito de impedir u obstaculizar su normal uso o funcionamiento, o a sabiendas de que puede producirse este resultado, destruya, altere, dañe o perjudique en cualquier forma los medios, recursos, edificaciones, instalaciones o unidades socioeconómicas o militares siguientes:
a. fuentes energéticas, obras hidráulicas, servicios de transporte terrestre, de comunicaciones y de difusión;
b. talleres, frigoríficos, depósitos, almacenes u otras instalaciones destinadas a guardar bienes de uso o consumo;
c. centros de enseñanza, edificaciones públicas, comercios, albergues o locales de organizaciones administrativas, políticas, de masas, sociales o recreativas;
ch. centros industriales o agropecuarios, cosechas, bosques, pastos o ganado;
d. instalaciones portuarias o de aeronavegación, naves o aeronaves;
e. centros de investigación, cría o desarrollo de especies de animales;
f. campamentos, depósitos, armamentos, construcciones o dependencias militares en general.

[64] QUINTERO OLIVARES, PEDRO. Comentarios a la parte especial del derecho penal. Ed. Arazandi. 2ª edición. España. Pamplona. 1999. p. 110.

propiamente dicha, mientras que las segundas tienden al agotamiento de la conducta delictiva, al hacer efectivas la inseguridad en el tráfico monetario internacional.

Ha de entenderse como acto de fabricación, la confección a partir de diferentes materiales de un objeto a imitación de cualquier moneda de curso legal que presente visos de autenticidad. Sin embargo, no basta con la mera imitación del objeto, sino que además será necesario que tal imitación sea lo suficientemente parecida al original como para engañar al hombre medio, es decir ha de ser idónea para el engaño, la no autenticidad de la moneda ha de pasar por alto a personas no expertas[65].

La consumación de la creación de moneda apócrifa, tanto por fabricación como por alteración, se produce en el momento en que se termina la confección de la moneda, sin ser necesario que ésta se haya introducido en el tráfico jurídico aunque sí ha de ser idónea para su introducción, ni que se haya producido perjuicio a alguien. Se trata pues, de un delito de resultado que permite la tentativa.

Falsificación de documentos.

El tipo objetivo del delito, sustentado en los verbos rectores: confeccionar, contribuir, intercalar, suprimir, ocultar, destruir y usar, hacen que el sujeto activo puede resultar cualquier persona, sea ésta un funcionario o un particular, y que su ejecución no puede ser de forma imprudente. Cabe tanto la falsificación ideológica como la material. Mientras que la consumación no exige de un resultado, basta con la ejecución de la conducta típica.

[65] Señala al respecto, Cuello Calón, E., op. cit., p. 193, que "La moneda metálica ha de tener la apariencia de moneda legítima. Su imitación ha de alcanzar un grado de perfección suficiente para que el público en general la tome por verdadera, bastante para que sea susceptible de ser puesta en circulación, más no es preciso que la semejanza con la moneda legítima sea tal que llegue a engañar a los mismos técnicos. Si la imitación es tan tosca e imperfecta que la falsedad sea por todos perceptible, el hecho no podrá integrar un delito consumado." Mientas que, "Respecto a la fabricación de papel moneda falso son aplicables los mismos criterios relativos a la moneda metálica: que el billete falso tenga la apariencia de legítimo sin que sea precisa una absoluta semejanza, basta que pueda inducir a error acerca de su legitimidad, que sea adecuado para poder circular entre el público como legítimo. Cuando el billete fabricado fuera tan tosco e imperfecto que no tuviere aspecto de legitimidad el hecho podrá constituir un delito frustrado o tentativa."

Fabricación, introducción o tenencia de instrumentos destinados a falsificar.

Conforme puede apreciarse de la conducta típica que se establece, sustentada en los verbos rectores de fabricar, introducir y tener, el delito no puede cometerse por imprudencia[66]. Así como tampoco es viable, por su propia esencia típica la tentativa y la conducta que se describe es evidentemente dolosa. En relación con algunos delitos concretos, el legislador ha estimado que la evidencia deducida de la fabricación o la tenencia de ciertos útiles o instrumentos de una potencial conducta delictiva aconseja anticipar la intervención del derecho punitivo, lo cual no podría en ningún caso conseguirse forzando el concepto de inicio de la ejecución para así adelantar la posible intervención del derecho penal, aunque fuera con infracción de la definición legal de la tentativa, lo cual, lógicamente no se puede hacer.

Sin embargo, habrá de tenerse cuidado al enjuiciar respecto a dicha conducta delictiva, en un sentido o en otro, por cuanto los referidos instrumentos o útiles pueden ser legítimos en poder de sus titulares legales, por lo que la ilegitimidad no depende sólo de la naturaleza del objeto, sino de eso unido a la legalidad de su utilización posible.

3.1.3 - Delitos contra la economía nacional.

Estos delitos están relacionados con la llamada delincuencia económica y con el contenido del llamado Derecho Penal Económico que es el conjunto de normas mediante las cuales el Estado procura proteger con el instrumento del Derecho Penal las reglas de funcionamiento de su sistema económico partiendo de una definición que le obligará a determinar aquellos bienes jurídicos que deben ser expresamente protegidos con una norma penal.

Actividades económicas ilícitas.

Se parte del principio que para realizar cualquier tipo de actividad económica con fines de lucro tiene que estar expresamente autorizada por una disposición legal o reglamentaria y

[66] Ley No 62. Código Penal. Cuba. Artículo 259. 1: El que fabrique o introduzca en el país cuños, prensas, marcas u otra clase de útiles o instrumentos destinados conocidamente a la falsificación de que se trata en las secciones anteriores, es sancionado con privación de libertad de dos a cinco años.

en el caso que este autorizado tener la licencia correspondiente, de lo contrario puede cometerse el presente delito. El elemento material de la acción se caracteriza por la realización de una acción o una pluralidad o repetición de tales actos ilícitos, en un relativo espacio de tiempo, sin que ello signifique necesariamente habitualidad o dedicación.

Los incisos 2[67] y 3 abordan dos circunstancias de agravación específica, una cuando se contrata mano de obra o se utilicen medios o materiales de procedencia ilícita aun en el caso que se tenga licencia o de cualquier forma se incumpliera lo establecido en los reglamentos para obtener mayores ganancias.

Por otra parte de acuerdo al inciso 4 del presente artículo no puede ser una actividad de reducida significación económica, evaluándose esto por la autoridad actuante, se exceptúan los casos en que se contrate mano de obra o cuando se realice con medios o materiales de producción ilícita.

La provincia investigó un caso tramitado por el delito de Actividad Económica Ilícita donde existe presencia del uso de las TIC como medio y fin para materializar esta acción, en el fueron encartados tres individuos confesos de los hechos, a los cuales se les aplicó medida cautelar de prisión provisional, para materializar el mencionado hecho aproximadamente se les ocupó 200 piezas, dentro de ellas computadora, memoria flash, modem, accesorios de servidor, tarjetas de red, cable coaxial, controlador remoto, antena parabólica, disco duro, celular, entre otros, de ellas 90 quedó demostrado que se utilizaron en la comisión del delito y 100 no eran producto de la actividad ilícita y 10 eran de creación artesanal para construir los productos. Lograron materializar la venta de los productos elaborados (antenas parabólicas) obteniendo considerables sumas de dinero, se les practicó prueba testifica y pericial obteniendo resultados positivos. El nivel cultura de los individuos encartados es positivo: Licenciado en Cibernética y Matemática y Especialista Principal de una empresa informática, Operador de Micro y Chapistero; se demostró en dos de los acusados el dominio de las técnicas informáticas así como en el tercero las habilidades constructivas para confeccionar los productos. Se comprobó que los acusados

[67] Ley No 62. Código Penal. Cuba. Artículo 228. 2: Si para la realización de los hechos a que se refiere el apartado anterior se contratara mano de obra o se utilizaran medios o materiales de procedencia ilícita, la sanción es de privación de libertad de uno a tres años o multa de trescientas a mil cuotas o ambas.

son de buena conducta social, con vínculo laboral, sin antecedentes penales. Se decretó en el fallo la sanción de autor del delito de Actividad Económica Ilícita a tres años de privación de libertad, subsidiado a trabajo correccional sin internamiento, autor de mismo delito a cuatro años de privación de libertad, subsidiado a trabajo correccional sin internamiento y autor del delito de especulación con multa de doscientos cincuenta cuotas de diez pesos.

Tomando como base los hechos narrados anteriormente queda demostrado que el delito objeto de estudio tiene presencia del uso de las TIC pero no necesita modificaciones puesto que sus apartados llegan al fondo del asunto, pero como se explicará posteriormente es de las tipicidades que necesita al momento de encuadrar la sanción la atenuante o la agravante del uso de los medios telemáticos para poder ser más exacto.

3.1.4 - Delitos contra los derechos patrimoniales.

Estafa.

La estafa es un delito esencialmente intelectual y ello se debe a su naturaleza variable, pues son infinitos los medios por los cuales esta puede producirse; mediante esta se pueden obtener bienes muebles e inmuebles y todo tipo de ventajas, provechos, beneficios y lucros. Se corporifica cuando el sujeto, que es de carácter general en la figura básica, con el propósito de obtener para sí o para un tercero, una ventaja o un beneficio patrimonial ilegítimo y empleando cualquier ardid o engaño que induzca a error a la víctima, o determine a esta a realizar o abstenerse de realizar un acto en detrimento de sus bienes o de un tercero.

El tipo penal exige un propósito determinado que se refleja en la obtención de una ventaja o un beneficio patrimonial, por lo que es imprescindible la conciencia y la voluntad de engañar a la víctima para lograr el fin perseguido, y se constituye en un delito intencional[68].

[68] Ley No 62. Código Penal. Cuba. Artículo 334.1: El que, con el propósito de obtener para sí o para otro una ventaja o un beneficio patrimonial ilegítimo, y empleando cualquier ardid o engaño que induzca a error a la víctima, determine a este a realizar o abstenerse de realizar un acto en detrimento de sus

Malversación.

La palabra malversación procede del latín male versare: dirigir mal o mal utilizar algo y significa en general invertir ilícitamente los bienes ajenos que una persona tiene a su cargo en usos distintos de aquellos para los que están destinados[69].

Se considera que el bien protegido pudiera integrar la familia de los delitos contra la economía nacional, dada la especial protección de esta en la conformación del tipo, y teniendo además en cuenta que en ese título se protegen figuras delictivas como las del artículo 224 y 225, que también son una desviación en la protección de bienes determinados que les han sido confiados a un sujeto especial.

El sujeto viene obligado por su condición de tener "en razón del cargo" determinadas obligaciones, lo que significa una competencia específica que posibilite tener bienes bajo su disposición o custodia de posible manejo por su actividad, por lo tanto, no puede cometer el delito quien no tenga una relación directa con el bien dado, por las condiciones antes señaladas y que deben haber sido establecidas por alguna disposición administrativa. Por lo que es imposible que un sujeto, aún reuniendo los elementos que establece el tipo penal, pueda malversar bienes que otro administra, por ello es imprescindible una estrecha relación entre funciones y bienes protegidos.

La conducta típica se establece mediante la acción de apropiarse de bienes de propiedad estatal, o de propiedad de las organizaciones políticas, de masas o sociales, o de propiedad personal al cuidado de una entidad económica estatal o consentir que otro se apropie.

El carácter de administrador tiene que darse cuando el sujeto, en función del cargo que ostente este facultado administrativamente para disponer de los bienes. Ello significa

---

bienes o de los de un tercero, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.

[69] Ley No 62. Código Penal. Cuba. Artículo 336.1: (Modificado) El que teniendo por razón del cargo que desempeña la administración, cuidado o disponibilidad de bienes de propiedad estatal, o de propiedad de las organizaciones políticas; de masas o sociales, o de propiedad personal al cuidado de una entidad económica estatal, se apropie de ellos o consienta que otro se apropie, incurre en sanción de privación de libertad de tres a ocho años.

que el sujeto tiene como atribución legal, poder dar destinos correspondientes a los bienes, utilizar y distribuir estos según las normas que le han sido establecidas legalmente para su adecuada administración.

La conducta persigue la obtención de un beneficio o un enriquecimiento económico para el autor o un tercero, pues el verbo rector lleva consigo el ánimo de lucro. La penalidad del tipo establece una sanción de tres a ocho años de privación de libertad, por lo que se encuentra en el rango de una sanción media que posibilita incluso la aplicación en los casos correspondientes, de una sanción sustitutiva que no conlleve el internamiento.

Daños.

Este delito se dirige a menoscabar la cosa en su integridad, disminuyéndole o eliminándole su valor económico de cambio o utilitario. Se trata, en fin, de proteger la incolumidad de las cosas que son propiedad de otro o propias, cuando tengan un evidente valor para la colectividad.

La figura básica exige además que el objeto de protección sea, perteneciente a otro, es decir, ajeno, siendo válida la explicación ofrecida al inicio de este estudio. Se encuentran presentes varios verbos rectores: destruir, deteriorar e inutilizar,[70] puede decirse que la acción de dañar esta constituida por todo ataque[71] a la materialidad, utilidad o disponibilidad de las cosas, que elimine o disminuya su valor de uso o cambio.

El elemento subjetivo caracteriza a este delito, pues tiene que tratarse de un acto dirigido a causar un daño de la cosa en sí misma,[72] por lo que requiere de un dolo directo constituido por la voluntad de querer dañar la cosa en sí. La figura se consuma con la producción efectiva del daño pero pueden presentarse formas imperfectas del

[70] Según el Diccionario Jurídico: Destruye la cosa el que la deshace o arruina de manera total o parcial, alterando su naturaleza o estructura; deteriorar significa menoscabar la cosa, degradar la misma en su composición. La inutiliza quien aún sin alterar su naturaleza o estructura, consigue que la cosa deje de ser apta para la función a que estaba destinada.

[71] CREUS, CARLOS: *Ob. cit*. p. 573. Considera que se ataca la materialidad de las cosas cuando se altera su naturaleza, forma o cualidades; se ataca su utilidad cuando se elimina su aptitud para el fin o los fines a que estaba destinada o se disminuye esa aptitud; se ataca su disponibilidad cuando el acto del agente impide que el propietario pueda disponer de ella como consecuencia del acto.

[72] Es lo que en la doctrina penal se conoce le conoce como *damnum injuria datum*, es decir, un daño injuriosamente inflingido.

delito. La figura agravada contempla que se puede cometer por concurrir las circunstancias de considerable valor, cuya cuantía se ha establecido en una cifra mayor a tres mil pesos o de producir el hecho un grave perjuicio.

3.1.5 – Resolución 127 de 2007 del Ministerio de la Informática y las Comunicaciones. Reglamento de seguridad para las Tecnologías de la Información.

El presente Reglamento tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. El termino Seguridad de las Tecnologías de la Información utilizado en este reglamento esta relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos.

En su Capítulo VII sobre los incumplimientos se establece que toda persona natural o jurídica que incumpla lo dispuesto en la presente Resolución y en las disposiciones legales vigentes en la materia, estará sujeta a la aplicación de las siguientes medidas:

Invalidación temporal o definitiva de las autorizaciones administrativamente concedidas por el Ministerio de la Informática y las Comunicaciones al infractor, entre ellas, cancelación de licencias, permisos, autorizaciones, desconexión parcial o total de las redes privadas de datos y otras.

Suspensión y/o cancelación, temporal o definitiva, de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano.

Ocupación cautelar de los medios, instrumentos, equipamientos y otros utilizados para cometer la infracción, con la finalidad de disponer posteriormente el decomiso de los mismos, según proceda.

La aplicación de las medidas que correspondan, de conformidad con lo legalmente establecido.

Toda persona natural o jurídica sujeta a la aplicación de las medidas descritas anteriormente puede apelar ante el Ministro del Ministerio de la Informática y las Comunicaciones en el plazo de 30 días hábiles contados a partir de la fecha de aplicada la medida. A su vez el Ministro dispondrá de 90 días hábiles para dar respuesta a dicha reclamación. La decisión de esta última instancia será inapelable.

3.2 – Propuesta de modificaciones al tratamiento legal de la criminalidad informática.

La Sección Sexta del Capítulo Cinco de la adecuación de la Sanción del Código Penal contempla lo referido a las Circunstancias Atenuantes y Agravantes, específicamente el Artículo 53 en el que enumera las circunstancias agravantes que se tiene que tener en cuenta para mover los límites mínimos y máximos del marco sancionador una vez que se haya calificado el delito. El mismo adolece de la presencia o uso de las Tecnologías de la Informática y las Comunicaciones por lo que se propone que se cree un inciso que contemple lo referido al uso de medios tales como: equipos computacionales, sistemas, medios, programas, redes informáticas u otra Tecnología de la Información y de las Comunicaciones.

Para este análisis se parte de que el uso de las tecnologías puede estar presente en disímiles familias de delitos como un medio que facilite la comisión de dicha actividad por lo que esto permite que se pueda ajustar la sanción y pueda producir un resultado más efectivo. Además impide que se tenga que prever específicamente por cada figura delictiva y se contemple solo en aquellas que así lo requieran por su magnitud o trascendencia. (Ver Anexo 3 y 7)

Espionaje.

Se propone contemplar en los apartados del Artículo 97 correspondiente al delito de Espionaje lo referente al que con ánimo de apoderarse, usar, conocer, revelar, difundir; información, datos o programas con carácter de secreto contenida en un sistema informático o medios análogos o intercepte, interfiera, acceda, borre, modifique, inutilice dichos medios será objeto de sanción penal.

Se considera así puesto que la revelación de información de carácter sensible puede conllevar a resultados nefastos por lo que se propone que se le de un tratamiento diferenciado siendo así que el objetivo principal es la protección de la Seguridad del Estado. Se prevé que cualquier persona puede cometer el referido delito por lo que se le da una figura de tipo general concibiendo que tiene que estar presente el dolo o sea el ánimo de tener acceso a la información y publicarla.

El precepto contempla dos momentos primero los que van dirigidos a la publicación de la información previendo acciones como apoderarse, usar, conocer, revelar, difundir; en este se utilizan los datos como un medio para lograr una acción o un delito posterior y un segundo momento en el cual los datos son el fin principal del delito, estableciendo verbos rectores como interceptar, interferir, modificar, borrar, inutilizar; la acción principal va encaminada a inutilizar la presencia de los mencionados archivos. Se menciona que para ello se tienen que hacer uso de las Tecnologías de la Informática y las Comunicaciones o sus elementos análogos (dispositivos de información extraíble, celular, computadoras, redes; entre otros) (ver Anexo 4).

Sabotaje.

Se propone contemplar en los apartados del Artículo 104.1 correspondiente al delito de Sabotaje, lo referente al que con el propósito de vulnerar, eliminar, destruir, dañar, modificar, inutilizar; el funcionamiento de un sistema que utilice Tecnologías de la Informática y las Comunicaciones o sus componentes (Ver Anexo 4) o provea de servicios a otros sistemas mediante el uso de técnicas informáticas (virus, gusanos, bombas lógicas, hackeo) será objeto de sanción penal.

El objetivo principal de este apartado es la protección de los sistemas informáticos que por sus características pueden ser objeto de ataque o de acciones que impidan su correcto funcionamiento. El delito puede ser cometido por cualquier persona para vulnerar, eliminar, destruir, dañar, modificar, inutilizar; un elemento importante es el medio de cómo se materializa el delito; o sea haciendo el uso de técnicas propias de la informática, dentro de estas se pueden mencionar el uso de programas malignos: virus, gusanos, bombas lógicas, troyanos, el uso de técnicas de hackeo, craqueo, spanes;

incluso podrá ser objeto de sanción el funcionario que por negligencia, impericia, o desconocimiento facilite o cree condiciones a un agente para que pueda vulnerar el sistema informático.

Propaganda enemiga.

Se propone contemplar en los apartados del Artículo 103.1 referente a la Propaganda Enemiga el que haciendo uso de las Tecnologías de la Informática y las Comunicaciones (redes informáticas, páginas web, salas de chateo, redes sociales) incite, promueva, difunda, publique; mensajes, reflexiones, propagandas, imágenes, audio, videos cuyo contenido vaya en contra de los principios del Estado y sea con el objetivo de fomentar la desestabilización, será objeto de sanción penal.

El objetivo principal de este apartado es la represión a aquellos individuos que hagan uso de las posibilidades y servicios que brindan las Tecnologías de la Informática y las Comunicaciones para la difusión y publicación de la información con técnicas como el acceso a redes informáticas (Internet, Intranet) a salas de intercambio virtual, foros de debate, páginas web y que las utilicen para fomentar la desestabilización interna o llamar a la disidencia mostrando mensajes, documentos, criterios que vayan en contra de los principios del Estado, se debe tener en cuenta que aunque el uso de las posibilidades que brinda la tecnología sea de libre acceso no significa que sea objeto para cometer estas manifestaciones, dado que un mensaje o llamamiento en la red puede ser visualizado por una amplia gama de usuarios.

Fabricación, Introducción o Tenencia de Instrumentos destinados a Falsificar.

Se propone contemplar dentro de los apartados del Articulo 259.1 correspondiente a los Delitos contra la Fé Pública referente a la Fabricación, Introducción o Tenencia de Instrumentos destinados a Falsificar, el que por cualquier vía produzca, introduzca o tenga bajo su poder, útiles, materiales, instrumentos, programas de ordenador, medios telemáticos hacia el Territorio Nacional con el objetivo de cometer cualquiera de los delitos de falsificación y haga uso de los mismos contenidos en el Código Penal será objeto de sanción penal.

El desarrollo tecnológico a posibilitado que cada día se expandan más las posibilidades y las formas de crear falsificaciones más efectivas y exactas minimizando los riesgos de detección y error; siendo así la principal objetividad jurídica de este apartado es el uso de los medios informáticos para cometer los delitos de falsificación, reprimiendo al que por cualquier vía introduzca dichos medios ya que nuestro país al tener una economía subdesarrollada muchas de las tecnologías que se requieren para materializar estos delitos necesita ser importadas.

Estafa.

Se propone contemplar dentro de los apartados del Artículo 334.1 correspondiente a los Delitos contra los Derechos Patrimoniales referente a la Estafa que si el culpable se vale de la utilización de un medio telemático, aplicación o programa informático o un medio análogo será objeto de sanción penal.

El objetivo principal de este apartado es reprimir el uso de los medios informáticos para materializar el delito de estafa, teniendo presente que muchas veces el encartado se puede valer del desconocimiento de los usuarios que operan las tecnologías para poder cometer estas infracciones y pasar desapercibido.

Corroborando la anterior afirmación dentro de los casos investigados en la provincia de Sancti Spíritus se radicó un delito de Estafa de carácter continuado donde el autor, confeso de los hechos, para incrementar ilícitamente su patrimonio aprovechando las posibilidades que brinda la división de ETECSA en el territorio; realizó manipulaciones a líneas telefónicas en la cabecera provincial y en la provincia de Villa Clara para poder efectuar llamadas al exterior, por dicha acción cobraba una suma de dinero en moneda libremente convertible; siendo así la Empresa de Telecomunicaciones sufrió una pérdida aproximada a trece mil pesos en moneda nacional (13 000.00 CUP). Se demostró mediante prueba testifical, documental y pericial que el acusado aprovechando dicha situación creó una brecha en las líneas telefónicas para poder realizar llamadas al exterior consecuentemente con los daños y perjuicios que se arrojó con su actuar.

Malversación.

Se propone contemplar dentro de los apartados del Artículo 336.1 correspondiente a los Delitos contra los Derechos Patrimoniales referente a la Malversación, cuando el delito se comete por un funcionario o empleado de una entidad que haciendo uso de sus facultades se aproveche de los medios informáticos, modificando, creando, borrando, alterando; datos, información, programas con el objetivo de incrementar ilícitamente su patrimonio, será objeto de sanción penal.

En los momentos actuales en que el país digitaliza todas sus operaciones contables, se hace cada vez mas creciente y necesario la vigencia de una norma que reprima y sancione hechos delictivos que ataquen estos bienes, no es menos cierto que los programas que permiten digitalizar la contabilidad de las empresas, órganos e instituciones del Estado en disímiles ocasiones sufren de modificaciones que provocan grandes pérdidas; una vez descubierta estas fechorías ya ha pasado un término prudencial de tiempo por lo que la pérdida se ha acrecentado a tan altos niveles que resulta extremadamente difícil enmendar el daño; la insuficiencia de una legislación provoca que al encuadrar estos delitos quede un vacío y se determina calificarlos por otros que no tocan el fondo del asunto o muchas veces se archiva el proceso investigativo puesto que no hay elementos que resulten suficientes para la incriminación.

Teniendo presente la anterior argumentación se propone la modificación de dicho delito puesto que carece de elementos suficientes para incriminar a sus ejecutores, creando así una figura específica para el funcionario o empleado del estado que teniendo las condiciones, el tiempo, el conocimiento y las posibilidades cometa malversación adulterando los programas informáticos mediante acciones como borrar, modificar, alterar; siempre teniendo presente que el móvil de la acción es incrementar ilícitamente el patrimonio.

Dentro los casos investigados en la provincia hacia una de la entidades estatales se comprobó que el económico de dicha entidad aprovechando las posibilidades de su cargo instaló directamente un programa contable, comprado a una empresa que lo proporciona, creando así una base de datos unificada donde, violando la seguridad

informática con una clave de acceso de dominio general, se realizaban cambios frecuentes a los datos almacenados. A ello se le agregó una herramienta de trabajo, no contemplada en este programa, que paralizó la facturación de mercancías durante un término prudencial de tiempo.

Se propuso por el infractor la creación de una cuenta abierta por todos los subsistemas contables, a la que se podía entrar desde todo el sistema, al conocerse la clave del administrador económico, permitiendo transferir directamente mercancías entre almacenes y utilizarse además para limpiar la contabilidad y transferir faltantes entre unidades, al momento de estarse realizando cualquier inventario.

Todo ello conllevó a que la empresa sufriera una pérdida aproximada a ochocientos mil pesos en moneda nacional (800 000.00 CUP). Esta diferencia corresponde a pérdidas fijadas contablemente que no cuentan con expedientes, no estando depuradas las causas que las originan, ni los responsables.

Daños.

Se propone contemplar dentro de los apartados del Artículo 339.1 relativo al delito de daños lo referente al que intencionalmente destruya, deteriore o inutilice documentos electrónicos, datos, programas de computación, redes y sistemas informáticos, para ocasionar un perjuicio a una institución o a una persona en específico será objeto de sanción penal.

La dependencia que presenta la sociedad sobre el uso de las Tecnologías de la Informática y las Comunicaciones a propiciado que la pérdida y destrucción de la información conlleve a generar resultados desastrosos, por lo que se prevé una especial protección bajo el delito de daños a aquellas personas que con la intención de causar perjuicios creen las condiciones necesarias para influir sobre estos bienes que por su carácter de intangibilidad en muchas ocasiones no se pueden recuperar.

Como se ha expresado anteriormente los delitos que se relacionan con las Tecnologías de la Informática y las Comunicaciones tienen dos formas de expresión los que se utilizan como medio para realizar una actividad y los que se utilizan como fin, en este caso se generan nuevas formas de delinquir de las cuales el Código Penal no presenta

ninguna tipicidad.

Un elemento muy importante a tener en cuenta es la seguridad informática de los medios telemáticos la cual nos indica cuales son los principales componentes a proteger dentro de un sistema informático dentro de los que podemos mencionar el hardware, el software y los datos; estos constituyen la base sobre las que se sustentan otras aplicaciones y servicios como son las redes informáticas, los usuarios, los dispositivos extraíbles, el correo electrónico la navegación etc.

Delitos contra la seguridad informática.

Se propone crear un bien jurídico referente a la seguridad de las Tecnologías de la Informática y las Comunicaciones dado que la misma esta presente en todas las ramas donde se utilizan los medios informáticos y se vincula directamente con la presencia de un delito de esta índole así como sus vulnerabilidades pueden ser las causas y condiciones que propicien esta aparición; un ejemplo que demuestra severidad es el informe de causas y condiciones emitido por la Fiscalía en uno de los expedientes analizados donde quedó demostrado: Violaciones con claves de acceso de dominio público que propiciaban la realización de los balances contables fuera del horario laboral, instalación por personal no autorizado de programas contables, creando una base de datos unificada, que le permitía entrar y manipular los sistemas contables desde cualquier unidad y la propia empresa.

Siendo así se podrán contemplar los siguientes apartados:

Acceso no autorizado a los medios informáticos.

El que haga uso de los medios técnicos o de comunicación y sus soportes de información, sin el consentimiento de su titular, o sin estar autorizado poniendo en riesgo la confidencialidad, integridad, y disponibilidad de la información que se procesa, intercambie, reproduce o conserva o impida el acceso al mismo será objeto de sanción penal.

La Resolución 127 de 2007 del Ministerio de la Informática y las Comunicaciones

establece que para lograr confidencialidad de la información esta no debe ser revelada sólo a los usuarios autorizados, en la forma y tiempo determinado, entiende por integridad que la información no sea modificada, incluyendo su creación y borrado sólo por personal autorizado, y por disponibilidad, que la información sea utilizable cuando y como lo requieran los usuarios autorizados.

Este apartado se relaciona con el delito de daños puesto que se produce un perjuicio con los dos al titular, pero en este último anexamos un elemento importante que es sobre la base de la que se sustenta el apartado, el acceso no autorizado a los medios informáticos, que establece que este se materializa por alguien no autorizado explícitamente para ello, se puede tener acceso autorizado a un sistema y no tener derecho a acceder a determinadas áreas del mismo, por lo que se considera como una brecha que puede ser blanco para cometer delito.

Si los hechos descritos en el apartado anterior se cometen en redes, sistemas estatales, gubernamentales, de organizaciones comerciales o educativas nacionales o de país aprovechando brechas, huecos o negligencias del personal especializado la sanción aumentará su cuantía.

Uso de programas malignos.

El que sin la debida autorización, produzca, trafique, adquiera, destruya, introduzca o extraiga del territorio nacional o tenga en su poder programas de computación con fines dañinos, tales como, virus informático, caballo de troya, bomba lógica, gusano u otros análogos, será objeto de sanción penal. (Ver Anexo 6).

El programa maligno es una serie de códigos que el programador realiza con el fin de cumplir una tarea específica, son capaces de reproducirse a sí mismos sin que el usuario esté consciente de ello; se adicionan a programas de aplicación así como a componentes ejecutables del sistema, de forma tal que puedan tomar el control del mismo durante la ejecución del sistema infectado, no cumpliendo las medidas de seguridad informática establecidas en las normas correspondientes los resultados pueden ser desastrosos, por lo que se prevé una objetividad jurídica que reprima estas manifestaciones.

Intercepción de comunicaciones.

El que intencionalmente, sin la debida autorización o excediendo la que se le hubiere concedido, intercepte, interfiera, bloquee o use un sistema o red de computadoras, un soporte lógico, programa de computación o base de datos o cualquier otra aplicación informática, en todo o en parte incurre para dichos fines en sanción penal.

Si el hecho previsto en el Apartado anterior tiene por objeto procurar un beneficio indebido para si o para un tercero, la sanción aumentará su cuantía, como mismo el que por su negligencia o descuido de lugar a que un tercero no autorizado acceda, intercepte, interfiera o use un sistema o red de computadora, un soporte lógico, programa computarizado o base de datos o cualquier otra aplicación informática en todo o en parte. Las sanciones previstas en este título se imponen siempre que el hecho no constituya un delito de mayor cuantía.

El desarrollo de las comunicaciones ha posibilitado que se aumente la interdependencia entre los usuarios y el uso de las tecnologías, por lo que se prevé una figura específica que proteja y reprima estas conductas, son pocas las instituciones del Estado que no tienen hoy comunicación por correo electrónico, así como una red de computadoras de alcance, local, institucional, nacional o internacional que provea de servicios a los usuarios conectados; con acciones como interceptar, interferir, bloquear se puede lograr la caída de las comunicaciones entre las estaciones de trabajo y con ello provocar graves daños a la institución, en la mayoría de los casos son los servidores los principales blancos de ataque pues constituyen los procesos priorizados sobre los que se sustentan los servicios.

Como conclusión del desarrollo de este capítulo se evidencia la necesidad de las modificaciones que se proponen por el hecho de que la legislación actual como ha sido analizada con anterioridad no da respuesta al enfrentamiento a los delitos generados de la criminalidad informática, en la medida que la tecnología se desarrolle cada día más y alcance mas campos de acción en la sociedad los delitos irán evolucionando y se harán cada día más sofisticados, más difíciles de detectar y combatir y por supuesto provocarán más daños al país y a la sociedad.

Conclusiones

Como resultado de la investigación se arriban a las siguientes conclusiones:

Primera: El acelerado desarrollo y explotación de las Tecnologías de la Informática y las Comunicaciones ha propiciado que surja una nueva forma de delinquir catalogada como delito informático, todo ello derivado de la diversidad de conceptos ajustados al contexto de cada país y su campo de acción, que se caracterizan por su amplitud a todas las ramas de la sociedad, sus perpetradores y sus características que los diferencian de otros comisores, así como la forma de tipificarlos, prevenirlos y combatirlos.

Segunda: En análisis realizado a la estadística ofrecida por diferentes órganos que previenen y combaten esta conducta ha quedado demostrado que la tendencia de su comisión es a aumentar cada día más, con pluralidad de delitos y uso de medios, así como su respectiva afectación a la economía.

Tercera: En el contexto internacional son varios los países que contienen en su legislación figuras delictivas que sancionan la criminalidad informática, existiendo diversidad de tipicidades y sanciones. En cuanto a la forma de legislarlos la tendencia ha sido: enmarcarlos dentro del Código Penal, realizándole modificaciones a delitos tradicionales; crear un bien jurídico específico para estas tipicidades y elaborar una ley que reprima estas conductas delictivas.

Cuarta: La regulación que ofrece la normativa cubana al tratamiento de la criminalidad informática es insuficiente en relación al contexto actual de desarrollo de las mismas, dado que se tipifica por delitos tradicionales que no contemplan en sus apartados el uso de los medios telemáticos. Esto impone la necesidad de realizar modificaciones al Código Penal para lograr una correcta calificación y darle un tratamiento más efectivo, en particular a las figuras de sabotaje, espionaje, propaganda enemiga, malversación y daños, así como formular nuevas tipicidades al amparo de la seguridad informática, tales como el acceso no autorizado, el uso de los programas malignos y la intercepción de las comunicaciones.

Recomendaciones

Primera: Sugerir a las autoridades competentes considerar la necesidad de introducir modificaciones al Código Penal en materia de criminalidad informática con el objetivo de lograr lo siguiente:

- Especificar en la normativa el uso de los medios informáticos para cometer delito realizando modificaciones a figuras ya contempladas que se relacionan de forma directa, como el sabotaje, el espionaje, la propaganda enemiga, la malversación, los medios para cometer falsificación, los daños, y que se cree un bien jurídico nuevo relacionado con la seguridad informática y sus manifestaciones.

Segunda: Continuar el estudio de está temática, con una visión más amplia de cómo se manifiestan estas conductas en dependencia del desarrollo de las Tecnologías de la Informática y las Comunicaciones, que puedan incidir en la aparición de otras formas de cometer delitos dentro de la criminalidad informática.

Bibliografía

I. Textos.

1. Alfonso Toledo, José. *"Metodología de Investigación Criminalística para Casos de Perpetración de Delitos Informáticos".* Tesis de Grado. Chile. 2001. p. 328.
2. Amoroso Fernández, Yarina. *"La Informática como objeto de Derecho"*. Revista Cubana de Derecho. No. 1. Cuba. 1991. p. 45.
3. Arregoitia López, Siura L. *"Posibles Sujetos de los Delitos Informáticos"*. Facultad de Derecho. Universidad de La Habana. Cuba. 2009. p. 9.
4. Arregoitia López, Siura L. *"Protección contra los Delitos Informáticos en Cuba"***.** Facultad de Derecho. Universidad de La Habana. Cuba. 2009. p. 3.
5. Arregoitia López, Siura L. *"Rasgos afines de los llamados Delitos Informáticos"*. Facultad de Derecho. Universidad de La Habana. Cuba. 2009. p. 4.
6. Callegari, Lidia. *"Delitos informáticos y legislación"*. Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. No. 70 julio-agosto-septiembre. Colombia. Medellín. 1985. p.115.
7. Cordovés Rodríguez, Enrique. *"Características Generales de la Criminalidad Informática en Cuba"*. Cuba. Ciudad de La Habana. 2006. p. 3.
8. Cordovés Rodríguez, Enrique. *"Definiciones sobre Delito Informático"*. Intranet MININT \ Web Delitos informáticos\ ismi.htm. Cuba. 2007.
9. Cordovés Rodríguez, Enrique. *"Manual de Enfrentamiento a la Criminalidad Informática".* Cuba. 2004. p. 10.
10. Defensa Nacional. *"Unidad, Independencia y Soberanía".* Colectivo de Autores. Colegio de Defensa Nacional. Ediciones Verde Olivo. Cuba. 1997. p. 39.
11. *Delitos Informáticos Reconocidos por Naciones Unidas.* Tabla Facultativa. Intranet MININT\ Web Delitos Informáticos\ ismi.htm. Consultada. 2007.
12. *Derecho Penal Parte Especial*. Colectivo de Autores. Tomo I. Cuba. 2003.
13. *Diccionario Encarta.* Enciclopedia Microsoft. Encarta 2009.
14. Estebes García, Lidia. *"Particularidades de las conductas criminógenas donde se involucran las Tecnologías de la Informática en el contexto de las personas jurídicas".* Tesis de Maestría. Cuba. Ciudad de La Habana. 2009. p.50.

15. Estrada Garavilla, Miguel. *"Delitos Informáticos".* Universidad Abierta. http://www.universidadabierta.edu.mex. México. 2008. p. 16.
16. Fernández Calvo, Rafael. *"El tratamiento del llamado "delito informático" en el proyecto de ley Orgánico del Código Penal; reflexiones y propuestas de la CLI"*. Comisión de Libertades e Informática en Informática y Derecho. p.1150.
17. García García, Alejandro. *"Informática Jurídica y Derecho Informático"*. Cuba. 2006. p. 11.
18. Hernández Claudio. *"Hackers. Los piratas del Chip y de Internet"*. Ed. Mc Graw Hill. México. 2001. p. 101.
19. Hernández Sampieri, Roberto. *"Metodología de la Investigación"*. Segunda edición. Ed. Mc Graw Hill. México. 2006.
20. Herrera Bravo, Rodolfo. *"Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la Ley Chilena No. 19. 223"*. Chile. Santiago de Chile. 2003. p. 76.
21. Huerta Miranda, Marcelo y Claudio Libano Manssur. *"Delitos Informáticos"*. Ed. Jurídica Cono Sur. Chile. Santiago de Chile. 1998.
22. Lima de la Luz, María. *"Delitos Electrónicos en Criminalia"*. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio. México. 1984. p.100.
23. López Díaz, Claudia. Traductora. Versión publicada bajo el título Strafgesetzbuch, 32a, edición, Deutscher Taschenbuch Verlag, C. H. Beck, Munich, 1998. Fuente: http://jurcom5.juris.de/bundesrecht/stgb/index.html, actualizado hasta el 30 de agosto de 2002. *Código Penal del 15 de mayo de 1871* (RGBl. S. 127), en la versión del 13 de noviembre de 1998 (BGBl. I, 3322), modificada últimamente 34a Ley modificatoria del derecho penal: *§ 129b StGB (34. StrÄndG)* vom 22. August 2002 (BGBl. I, 3390).
24. Naciones Unidas. Revista Internacional de Política Criminal. Nos. 43 y 44. Naciones Unidas. Nueva York. 1994. p. 50.
25. Quintero Olivares, Pedro. *"Comentarios a la parte especial del derecho penal"*. Ed. Arazandi. 2ª edición. España. Pamplona. 1999. p. 110.
26. Ramírez Bejerano, Emilio y Ana Rosa Aguilera Rodríguez. *"Los delitos informáticos"*. Tratamiento internacional. Cuba. 2009. p. 10.
27. Reyna Alfaro, Luis M. *"Aproximaciones victimológicas al Delito Informático"*. Capítulo Criminológico Vol. 31. Nº 4. 93-104ISSN: 0798-9598. Universidad de San Martín de

Porres. Universidad Nacional Mayor de San Marcos. Perú. Lima. Octubre-Diciembre 2003. p. 5.

28. Sarzana, Carlos. *"Criminalita e Tecnología en Computers Crime; Rassagna Penitenziaria e Criminología"*. Nos. 1-2 Año 1. Italia. Roma. p.53.
29. Sutherland, Edwin. *"Teoría de la Criminología"*. Estados Unidos de América. Washington. 1943. p. 10.
30. Téllez Valdés, Julio. *"Derecho Informático"*. Instituto de Investigaciones Jurídicas. Ed. Mc Graw Hill. Interamericana de México S.A. México. 1997. p. 103 - 104.
31. Toledo Dumenes, José Alfonso. *"Delitos emergentes en Internet y el desafío de los carabineros de chile en la prevención y control en la era informática"*. Chile. 2007. p. 8.
32. Vega Vega, Juan. *"Los Delitos"*. Ediciones Estudios. Instituto Cubano del Libro. Cuba. La Habana.1968. p. 2.
33. Wikipedia, la enciclopedia libre. http://es.wikipedia.org.

II. Legislación.

1. *Acta de privacidad en las comunicaciones electrónicas*. Estados Unidos. 1986.
2. *Acta Federal de abuso computacional.* Estados Unidos. 1994.
3. *Código Penal Federal*. México. 1931.
4. *Decreto No. 17-73*. Código Penal. Guatemala. 1973.
5. *Ley No 8819 sobre el fraude informático*. Francia. 1988.
6. *Ley contra criminalidad económica que reforma el Código Penal*. Alemania. 1986.
7. *Ley contra delitos informáticos*. Holanda. 1993.
8. *Ley de reforma del Código Penal*. Austria. 1987.
9. *Ley Especial contra delitos informáticos*. Venezuela. 2001.
10. *Ley Federal de protección de datos personales*. México. 2003.
11. *Ley Federal de protección de sistemas*. Estados Unidos. 1985.
12. *Ley No 1273 sobre delitos informáticos*. Colombia. 2009.
13. *Ley No 19223 sobre delitos informáticos*. Chile. 1993.
14. *Ley No 26.388. Reforma del Código Penal*. Argentina. 2008.
15. *Ley No 8148. Reforma del Código Penal*. Costa Rica. 2001.
16. *Ley No. 62. Código Penal*. Cuba. 1988.

17. *Ley Orgánica de protección de datos de carácter personal (LOPD).* España. 1992.
18. *Ley Orgánica No 10*. Código Penal. BOE número 281, de 24 de Noviembre de 1995. España. 1995.
19. Resolución 127. *Reglamento de seguridad para las Tecnologías de la Información. Ministerio de la Informática y las Comunicaciones*. Gaceta Oficial No. 057 Ordinaria de 30 de agosto de 2007. Cuba. 2007.

III. Sitios en Internet.

1. http://biblioteca.usac.edu.gt/tesis/08/08_7985.pdf
2. http://delitosinformaticos.com/legislacion/espana.shtml. 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).
3. http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico. Delito Informático.
4. http://europa.sim.ucm.es/compludoc/AA?articuloId=119109&donde=castellano&zfr=0
5. http://lawiuris.wordpress.com/2009/06/02/el-delito-informatico/. Daniel Ernesto Peña Labrin. El Delito Informático y la Ius Cibernética.
6. http://vecam.org/article659.html. Stephani Carrin. Delito Informático.
7. http://www.alfa-redi.org/rdi-articulo.shtml?x=10653. Andrés San Juan. Comentario sobre la Ley de Delitos Informáticos. Junio. 2008.
8. http://www.alfa-redi.org/rdi-articulo.shtml?x=1387
9. http://www.alfa-redi.org/rdi-articulo.shtml?x=7178. Elena Pérez Gómez. Como actuar mediante la informática forense mediante delitos informáticos.
10. http://www.betsime.disaic.cu/secciones/jur_nd_03.htm. Lic. Marta Valdés Domínguez Asesora Jurídica. Casa Consultora DISAIC. Los Delitos Informáticos a la luz del Siglo XXI.
11. http://www.cabinas.net/informatica/delitos_informaticos.asp. Luciano Salellas. Delitos Informáticos y Ciberterrorismo.
12. http://www.delitosinformaticos.com/delitos/colombia3.shtml
13. http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml. Alicia Chiaravalloti. Introducción a los delitos informáticos, tipos y legislación. 2002.

14. http://www.delitosinformaticos.info/delitos_informaticos/definicion.html. Definición de delitos informáticos. Características principales.
15. http://www.derechoinformatico.com/
16. http://www.ecured.cu/index.php/Proteccion_contra_delitos_informaticos. Protección contra los delitos informáticos.
17. http://www.eumed.net/rev/cccss/04/rbar2.htm. Egil Emilio Ramírez Bejerano. Delitos Informáticos. Tratamiento Internacional.
18. http://www.fder.edu.uy/contenido/idi/biblio_integrantes.html
19. http://www.hfernandezdelpech.com.ar/ProyectosYanteproyectosArgProyLeyModifCodigoPenalIncorpoDelitosInfor.htm. Ley 26388 - Modificación del Código Penal. Delitos Informáticos. Sancionada el 4 de junio de 2008. Promulgada de hecho el 24 de junio de 2008. B.O. 25.06.2008.
20. http://www.ieid.org/congreso/ponencias/Reina%20Alfaro,%20Luis%20M.pdf
21. http://www.infoleg.gov.ar/infolegInternet/anexos/140000.htm. Código Penal. Ley 26.388. Argentina. 2008.
22. http://www.informatica-uridica.com/trabajos/trabajosDelitoInformatico.asp. Revista Jurídica Informática. Crímenes de Informática. Posibles sujetos de los delitos informáticos. Rasgos afines de los llamados delitos informáticos.
23. http://www.iuspenalismo.com.ar/doctrina/informaticos.htm. Adiestrarán a Fiscales sobre delitos informáticos.
24. http://www.lavozdelsandinismo.com/ciencia-tecnica/2010-062/adiestraran-a-fiscales-sobre-delitos-informaticos/. Carlos Alberto Pajuelo Beltrán**.** Gestión dogmática del Bien Jurídico Tutelado en los Delitos Informáticos en el Perú.
25. http://www.legifrance.gouv.fr/html/codes_traduits/penal_textE.htm
26. http://www.mailxmail.com/curso-delitos-informaticos/legislacion-sobre-delitos-informaticos-panorama-general
27. http://www.microsoft.com/business/smb/ess/legal/informatica_forense.msp. Como actuar ante delitos informáticos dentro de la empresa.
28. http://www.monografias.com/trabajos6/delin/delin.shtml. Mlandav. Delitos Informáticos.
29. http://www.pensamientopenal.com.ar/01022010/doctrina06.pdf

30. http://www.revistaciencias.com/publicaciones/EkpuFEVpVpdivwIXpH.php. Mailín Ochoa Calzadilla. Dilemas éticos de la Informática.
31. http://www.revistas.luz.edu.ve/index.php/cc/article/view/567/533
32. http://www.sabetodo.com/contenidos/EEVFFupFuZPNQaqBzb.php. Medrado López García. La protección de los derechos y libertades en el delito informático.
33. http://www.segu-info.com.ar/delitos/delitos.htm. Legislación y Delitos Informáticos.
34. http://www.segured.com/index.php?od=2&article=193. Milthon Chaves. Prevención de Delitos Informáticos.
35. http://www.slideshare.net/guest0b9717/robos-y-fraudes-informticos-presentation
36. http://www.terragnijurista.com.ar/doctrina/delinfo2.htm
37. http://www.tuabogadodefensor.com/01ecd193e810f1e01/Penal/index_dinform.htmPodemos incurrir involuntariamente en un delito informático.
38. http://www.venelogia.com/ex/tag/Delitos+inform%E1ticos
39. http://www.viegasociados.com/publicac/DelitosInformaticos.pdf
40. http://www1.universia.net/CatalogaXXI/C10046PPPEII1/E83648/index.html

Anexo 1: Reseña histórica del desarrollo de la Informática.

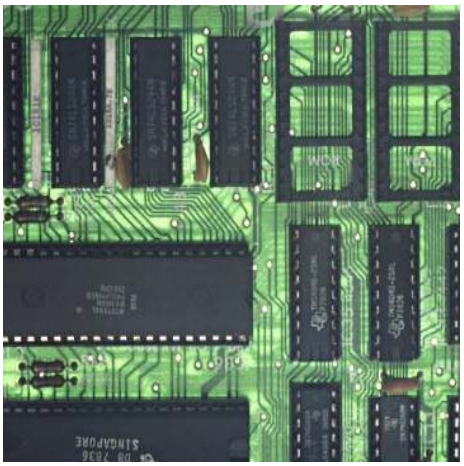
1ª Generación (1938-1952, 56)

Máquinas basadas en válvulas al vacío. ENIAC (Eckert-Mauchly) primer computador. En 1947 se construyó en la Universidad de Pennsylvania la ENIAC (Electronic Numerical Integrator and Calculator) que fue la primera computadora electrónica. El equipo de diseño lo encabezaron los ingenieros John Mauchly y John Eckert. Esta máquina ocupaba todo un sótano de la Universidad (un cuarto de 6 x 12 ms.), tenía más de 18 000 tubos de vacío, 70 mil resistencias. 7500 interruptores, su sistema de trabajo lo constituían 20 registros de 10 dígitos, consumía 200 Kw de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo.

2ª Generación (1953-1962, 63)

En esta generación las computadoras se reducen de tamaño y son de menor costo. Aparecen muchas compañías y las computadoras eran bastante avanzadas para su época como la serie 5000 de Burroughs y la ATLAS de la Universidad de Manchester. La segunda generación surge cuando se sustituye la válvula al vacío por el transistor. Se corresponde con la aparición de los primeros ordenadores comerciales. Estos ordenadores ya permitían interpretar instrucciones escritas en lenguaje de programación como Cobol o Fortran.

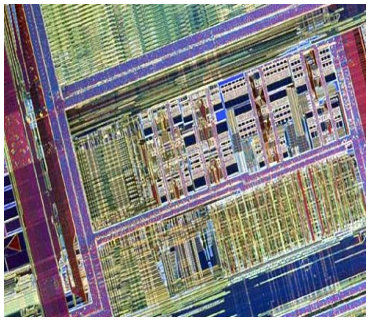
3ª Generación (1963-1971)



Con los progresos de la electrónica y los avances de la comunicación con las computadoras en la década de los 60, surge la *tercera generación* de las computadoras. Se inaugura con la IBM 360 en abril de 1964. La tercera generación va de 1964 a 1971 y se caracterizó por la utilización del circuito integrado como soporte de la información. Esto permitió abaratar los costos, reducir el tamaño de los ordenadores y aumentar sus prestaciones. Paralelamente se mejoraron los lenguajes de programación y empezaron a aparecer programas comerciales. IBM 360, el primer computador basado en circuitos integrados: 760. Aguantaban 20 terminales y podían encenderse varias veces al día.

Compatibilidad. La IBM, dice a sus clientes que los programas antiguos correrán en los nuevos modelos. Las empresas que compiten con la IBM, recibieron las características estándar, de sus equipos para satisfacer al mercado. PDP-8, PDP-11, de DEC, Modelos de Compatibilidad, supercomputadoras CDC7600 (1969). Ferrita por circuitos integrados para la memoria del computador. Programas que aparecen: Basic y Pascal.

4ª Generación (1972-1987)



Con la aparición del microprocesador que es la integración de todos los elementos básicos del ordenador en un solo circuito integrado surge la cuarta generación. Esta época se caracteriza por la mejora sustancial de los periféricos así como la aparición de lenguajes y herramientas informáticas. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada ***"Revolución Informática"*.**

En 1976 Steve Wozniak y Steve Jobs inventan la primera microcomputadora de uso masivo y más tarde forman la compañía conocida como la Apple que fue la segunda compañía más grande del mundo, antecedida tan solo por IBM; y esta por su parte es aún de las cinco compañías más grandes del mundo.

En 1981 se vendieron 800 000 computadoras personales, al siguiente año la cifra aumentó a 1 400 000. Entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no quedan dudas que su impacto y penetración han sido enormes.

Con el surgimiento de las computadoras personales, el software y los sistemas que con ellas se manejan han tenido un considerable avance, porque han hecho más interactiva la comunicación con el usuario. Surgen otras aplicaciones como los procesadores de palabra, las hojas electrónicas de cálculo, paquetes gráficos, etc. También las industrias del Software de las computadoras personales crecen con gran rapidez. Gary Kildall y William Gates se dedicaron durante años a la creación de sistemas operativos y métodos para lograr una utilización sencilla de las microcomputadoras (son los creadores de CP/M y de los productos de Microsoft).

No todo son microcomputadoras, por supuesto, las minicomputadoras y los grandes sistemas continúan en desarrollo. De hecho las máquinas pequeñas rebasaban por mucho la capacidad de los grandes sistemas de 10 o 15 años antes, que requerían de instalaciones costosas y especiales, pero sería equivocado suponer que las grandes computadoras han desaparecido; por el contrario, su presencia era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria. Las enormes computadoras de las series CDC, CRAY, Hitachi o IBM por ejemplo, eran capaces de atender a varios cientos de millones de operaciones por segundo.

5ª Generación (1981 -)

De 1981 hasta nuestros días se habla de la quinta generación que además de continuar el desmedido avance electrónico, se presta mucha mayor atención al software para acercar el ordenador a la forma de comunicación natural de un sujeto humano. Además en esta época aparece un tipo de ordenador que va a revolucionar el concepto de la

informática, el PC (Personal Computer). En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras.

Surge la competencia internacional por el dominio del mercado de la computación, en la que se perfilan dos líderes que, sin embargo, no han podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora en un lenguaje más cotidiano y no a través de códigos o lenguajes de control especializados. Japón lanzó en 1983 el llamado “programa de la quinta generación de computadoras”, con los objetivos explícitos de producir máquinas con innovaciones reales en los criterios mencionados. Y en los Estados Unidos ya está en actividad un programa en desarrollo que persigue objetivos semejantes, que pueden resumirse de la siguiente manera:

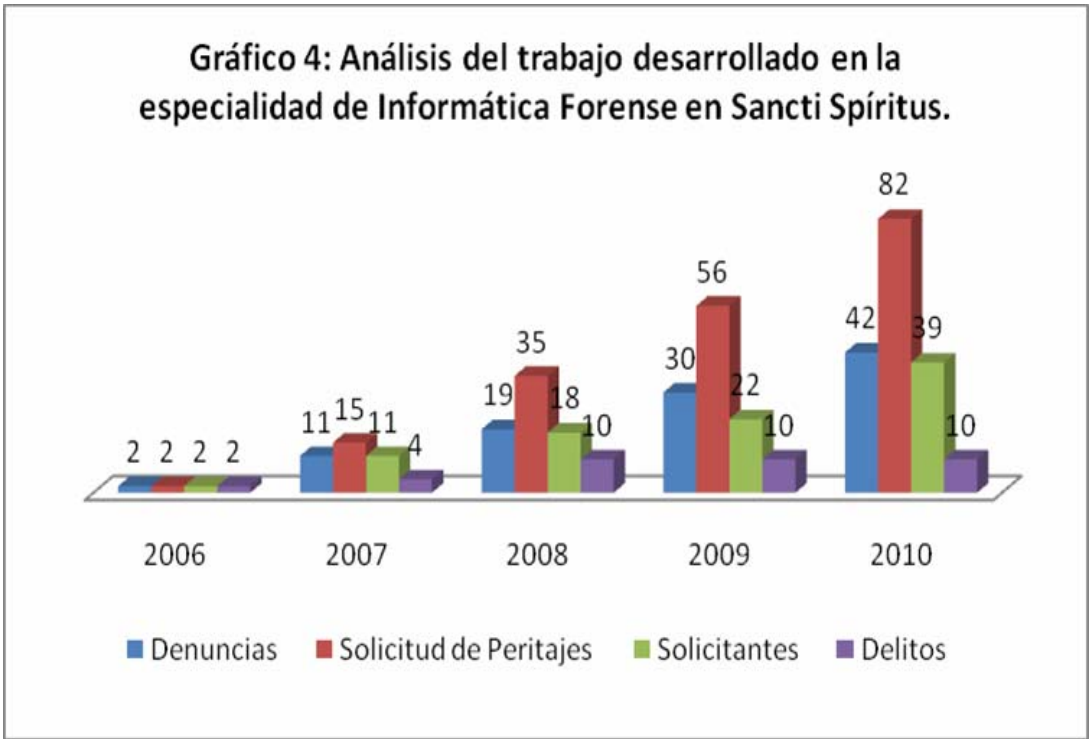
- Procesamiento en paralelo mediante arquitectura y diseños especiales y circuitos de gran velocidad.
- Manejo de lenguaje natural y sistemas de inteligencia artificial.

El futuro previsible de la computación es muy interesante, y se puede esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.

Anexo 2: Estadística del trabajo desarrollado en la especialidad de Informática Forense en Sancti Spíritus.

Año	Denuncias	Solicitud de Peritajes	Delitos	Órganos solicitantes	Evidencias
2006	2	2	2	2	14
2007	11	15	4	11	504
2008	19	35	10	18	46
2009	30	56	10	22	49
2010	42	82	10	39	251

Fuente: Laboratorio Provincial de Criminalística. 2011.

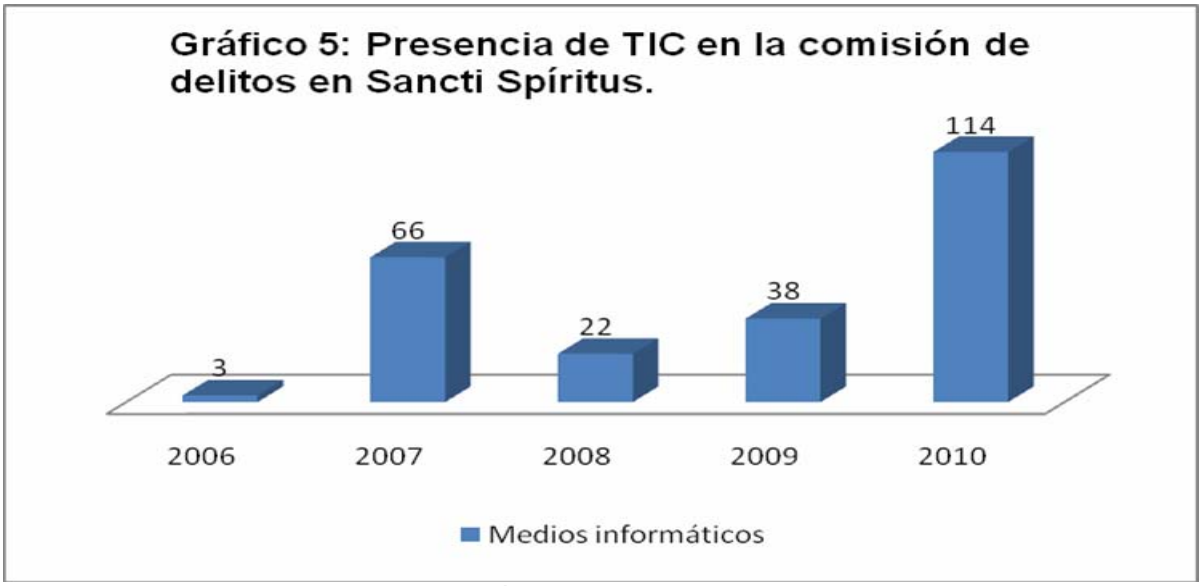


Fuente: Laboratorio Provincial de Criminalística. 2011.

Anexo 3: Presencia de Tecnologías de la Informática y las Comunicaciones en la comisión de delitos en Sancti Spíritus.

Medios Informáticos	2006	2007	2008	2009	2010
Computadora de Escritorio	1	16	1	9	6
Cámara digital	1	0	2	3	4
Disco CD	1	32	4	0	48
Disco Duro	0	2	0	1	22
Fuente Interna de Alimentación	0	1	0	0	1
Disco DVD	0	12	0	0	0
Celular	0	3	14	22	16
Teléfono	0	0	1	1	1
Memoria Flash	0	0	0	1	1
Lapto	0	0	0	1	3
Trazas de Servidor	0	0	0	0	2
Impresora	0	0	0	0	3
Disco Externo	0	0	0	0	1
Motherboard	0	0	0	0	2
Lector de CD	0	0	0	0	4
Total	3	66	22	38	114

Fuente: Laboratorio Provincial de Criminalística. 2011.



Fuente: Laboratorio Provincial de Criminalística. 2011.

Anexo 5: Guía de análisis de expediente de fase (datos del hecho)

FORMULARIO DEL EFP

No EFP:		Órgano:	
No Denuncia:		Dpto:	
Registro Salida:		Sección:	
Cant. Encartados:		Sección:	
Nombre del caso:		Prov/Municipio	
Gdo, Nombre Instructor:		Fiscal:	

Radicación Provisional:		Radicación Final:
Fecha Apertura:		Medida Cautelar aplicada
Fecha Cierre:		
Prorroga 1:		
Piezas Ocupadas		

Prueba Testifical:	Si___ No___	Aporte:	Si___ No___
Prueba Documental:	Si___ No___	Aporte:	Si___ No___
Prueba Pericial:	Si___ No___	Aporte:	Si___ No___

Acciones y Diligencias realizadas:

Acción	Resultado	
	Positivo	Negativo

Modus Operandi:
Causas Condiciones:

1) Datos generales:

a) Número del Expediente y Causa: Exp_____/_____ Causa _____/_____.

b) Identificado Si ___No ___ Habido _____ No Habido____.

2) Datos Personales de los implicados:

a) Carnet de Identidad:_____

b) Nombres_____Alias_____

c) 1er apellido:_____2do Apellido _____

d) Estado civil: Casado___, Soltero___ , Concubinato ___

e) Color de la piel: Blanca ___, Negra ___, Mestiza ___, Amarilla___

f) Edad:

- 16 ___ 16-20 ___ 21-25 ___ 26-30 ___ 31-35 ___ 36-40 ___ 41-50 ___ 51+ ___

g) Nivel cultural: Menos de 9no grado___, 9no grado___, 12 grado___, Técnico Medio___, Universitario___, Master___, Doctor en Ciencias____.

h) Vínculo escolar actual: Curso: _____

Institución: _____

i) Integración a las Organizaciones políticas y sociales:

1-CDR___ 2-MTT ___ 3-CTC ___ 4-ACRC ___ 5-UJC ___ 6-PCC ___.

j) Extracción Social: 1.Obrero __ 2.Campesino___ 3.Intelectual___ 4.Militar___

➢ Vínculo con la informática:

a) Nivel de instrucción en relación ala informática: institucional o autodidacta.

Institucional: Técnico Medio Informático___, Ingeniero Informático___, Cibernético____, Otros: ¿Cuál? _____

Autodidacta: Vía de capacitación: Cursos institucionales____, Cursos por Internet____, Cursos particulares ____.

b) Tipo de tecnología utilizada para prepararse: Propia _____, Institucional____

c) Vínculo escolar antes de ser procesado: Curso: _____

Institución: _____

3) Datos generales de la Persona Jurídica:

a) Nombre: _____,

b) Dirección:_____,

c) Municipio:_____, Provincia:_____,

d) Objeto social:_____,

e) Tipo de entidad: Nacional___, Extranjera___, Mixta___.

f) Forma de operación comercial: Moneda nacional___, Divisa____, Ambas____.

g) Nivel de las operaciones: Nacionales___, Internacionales___, Ambas ____.

h) Departamentos afectados: ¿Cuál? _____,

i) Procesos afectados: Productivos___, Financieros___, Servicios___,

j) Afectación económica: _____MN, _____Divisa

k) Resarcimiento: SI __, No__Tipo: Financiero___, moral___, prestigio____, otros _____

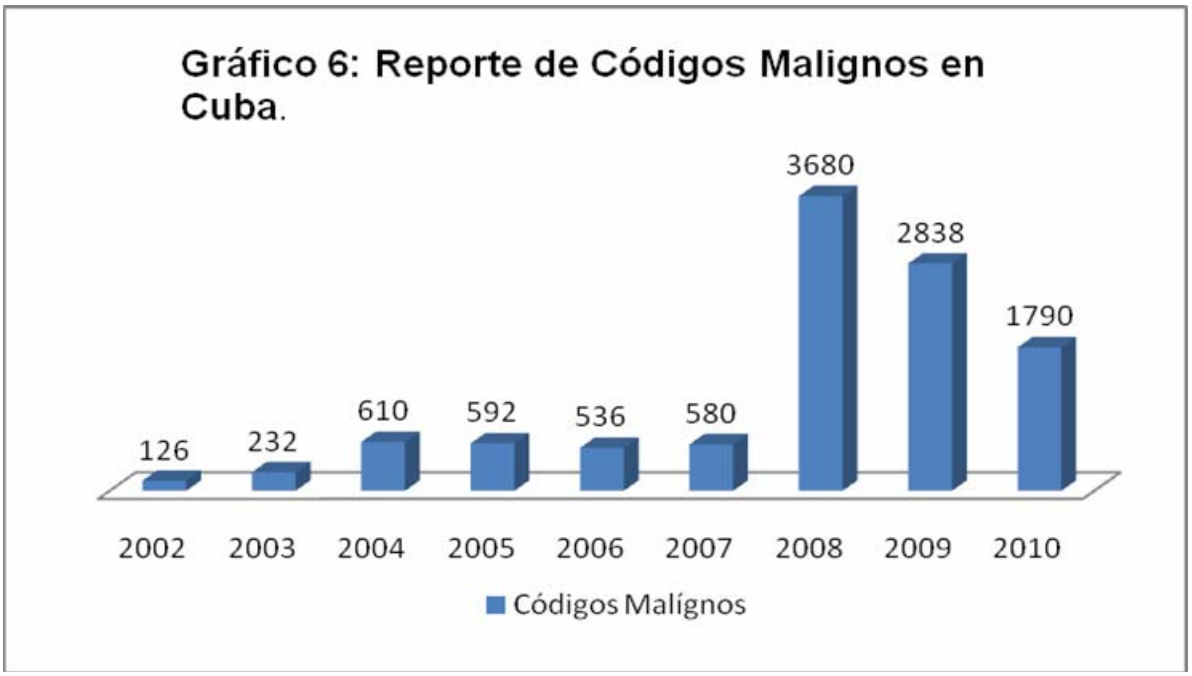
Fuente: Estebes García, Lidia. Particularidades de las conductas criminógenas donde se involucran las Tecnologías de la Informática en el contexto de las personas jurídicas. Tesis de Maestría. Cuba. Ciudad de La Habana. 2009.

Anexo 6: Reporte de Códigos Malignos detectados por Segurmática en Cuba.

En Cuba se han reportado 6024 programas malignos que corresponden a 421 Virus, 4216 Caballos de Troya, 1338 Gusanos, 24 Jokes y 25 Exploit los que se relacionan a continuación.

	2002	2003	2004	2005	2006	2007	2008	2009	2010
PROGRAMAS MALIGOS	63	116	305	296	268	290	1840	1419	895
VIRUS	9	11	12	8	10	9	18	1	3
CABALLOS DE TROYA	23	62	146	192	175	209	1362	1208	730
GUSANOS	25	43	126	91	76	72	459	210	162
JOKE	6	0	9	3	1	0	1	0	0
EXPLOIT	0	0	12	2	6	0	0	0	0
Total	126	232	610	592	536	580	3680	2838	1790

Fuente: http://www.segurmática.cu . 2011.

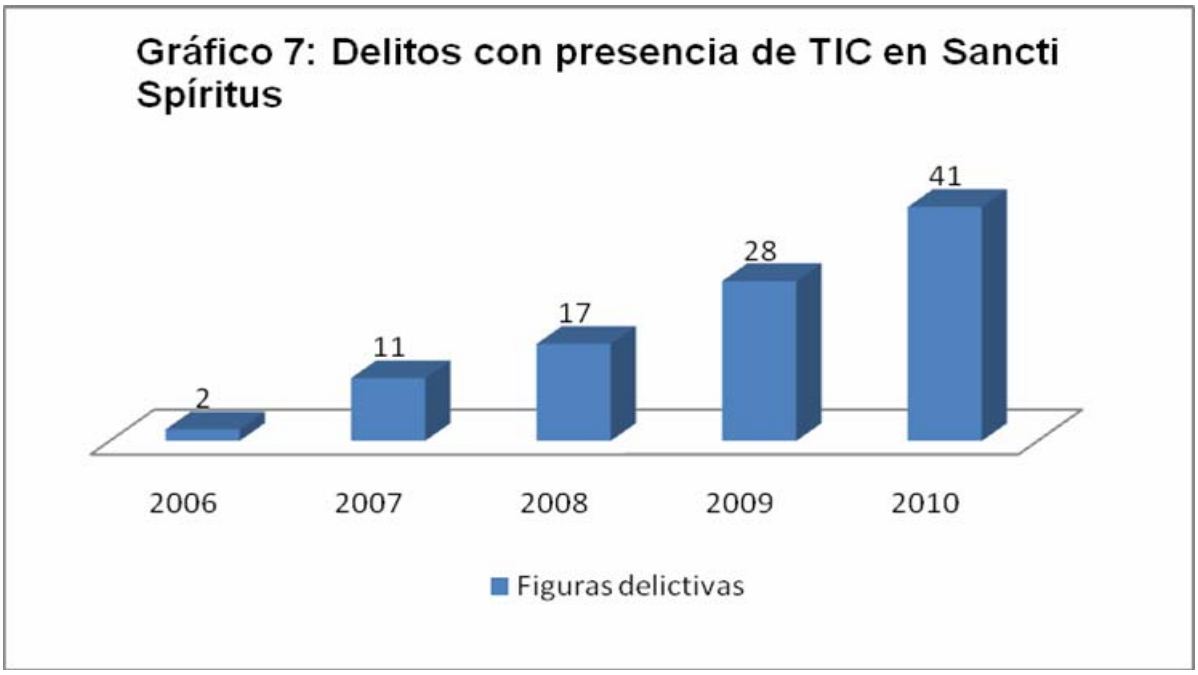


Fuente: http://www.segurmática.cu . 2011.

Anexo 7: Delitos cometidos con presencia de Tecnologías de la Informática y las comunicaciones en Sancti Spíritus.

Delito	2006	2007	2008	2009	2010
Hurto	1	0	1	0	3
Receptación	0	3	1	0	5
Contra Revolución	0	4	3	1	0
Drogas	0	1	0	0	3
Corrupción de Menores	0	0	2	1	0
Falsificación de Documentos	0	0	1	3	1
Robo con Violencia	0	0	1	2	0
Especulación y Acaparamiento	0	0	1	1	0
HSIGM	0	0	2	0	1
Hallazgo	0	0	0	1	0
Violación	0	0	0	2	0
Robo con Fuerza	0	0	0	0	2
Lesiones	0	0	0	0	1
Malversación	0	0	0	0	2
Estafa	0	0	0	1	0
Otros	1	3	2	14	23
Total	2	11	17	28	41

Fuente: Laboratorio Provincial de Criminalística. 2011.



Fuente: Laboratorio Provincial de Criminalística. 2011.