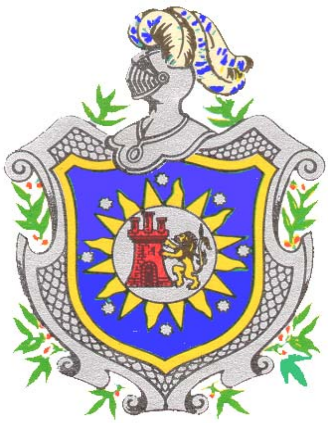
UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-LEÓN

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



TESIS PARA OPTAR AL TITULO DE

LICENCIATURA EN DERECHO

TEMA

LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL DE LA REPÚBLICA DE NICARAGUA

AUTOR

Br. EDUARDO AGUILERA MUÑOZ

TUTOR

LIC. LUIS HERNÁNDEZ LEÓN

León, Mayo del 2009.

AGRADECIMIENTO:

Agradezco a mi PADRE CELESTIAL DIOS, quien me brindó la vida, y quien con amor y mucha bondad me ha brindado el esfuerzo por concluir mi Monografía.

Dedico esta monografía a mis padres DIGNA ADA LUZ MUÑOZ Y HELIODORO AGUILERA VARELA, a quienes les debo mi existencia, mi educación y mis sueños, quienes me han brindado su apoyo incondicional, y por haber procurado siempre lo que en realidad ha sido lo mejor para mí.

No omito agradecer a mis hermanos Cesar Augusto Aguilera Muñoz, Lic. Carolina Aguilera Muñoz, Lic. José Luis Aguilera Muñoz, quienes me han apoyado en toda circunstancia de mi vida y me motivan a seguir superando en esta Vida.

Agradezco especialmente a mi maestro el Lic. Luis Hernández León, por haberme dedicado parte de su valioso tiempo, su apoyo, disposición y generosidad, y sobre todo por ser un buen tutor.

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

Br. Eduardo Aguilera Muñoz.

INDICE

Contenido ***Págs.***

Introducción……....1

Capitulo I DELITOS INFORMÁTICOS.

1.- Antecedentes……..……5
2.- Generalidades……..9
3.- Concepto……....11
3.1.- Típico……...…13
3.2.- Atípico……...…..14
4.- Características……...…..14
5.- Elementos de los Delitos Informáticos……..……16
5.1.- Elemento Objetivo……..……..…….16
5.2.- Elemento Subjetivo……..…....16
6.- Sujetos del Delito……..……..17
6.1.- Sujeto Activo……..17
6.2- Sujeto Pasivo……...…18
7.- Clasificación……...…..19
7.1.- Como Instrumento o Medio……20
7.2.- Como fin u objetivo……..21
7.3.- Tipos de Ataques contra los Sistemas de Información……..21
8.- Formas de control……..…..24
8.1- Preventivo……24
8.2- Correctivo……25
9.- Tipos de Delitos realizados por medios Informaticos reconocidos por la Organización de Naciones Unidas (ONU)……..26
9.1.- Otros Autores……30
9.2.- Otras clasificaciones……...31

Capitulo II TIPOS DE DELITOS REGULADOS EN EL NUEVO CÓDIGO PENAL

1.- Apertura o Interceptación Ilegal de Comunicación……35
2.- Estafa……36
3.- Daños……37
4.- Programas destructivos……38
5.- Delitos contra el Derecho de Autor y Derechos Conexos……39
6.- Reproducción ilícita……41
7.- Delitos contra las Señales Digitales……42
8.- Protección de Programas de Computación……44

Capitulo III BIENES JURÍDICOS TUTELADOS

1.- Derecho a la Privacidad e Intimidad……47
2.- Derecho a la Propiedad……52
3.- Propiedad Intelectual……54
4.- Derecho al Patrimonio……56
5.- Afectaciones a la Fe Pública……57
6.- Seguridad del Estado……58

Conclusiones……61

Bibliografía……66

INTRODUCCIÓN

El estudio de esta investigación en la que pretendido brindar una noción acerca de lo que son los Delitos Informáticos que hoy en día con la implementación del Código Penal de la Republica de Nicaragua, se encuentran dispersados en su articulado y que vienen a ser un aporte a la búsqueda del Delito Informático en el Derecho Penal Nicaragüense.

La magnitud de los Delitos Informáticos del nuevo Código Penal de la República de Nicaragua, es trascendente por el debido uso de los términos y/o conceptos del Derecho Informático, su naturaleza, su frecuencia puede dar un realce al impartir justicia con mano dura ante maniobras informáticas de la información, siendo manipulados por personas que buscan un beneficio propio y/o económico y que con el dolo, engaño, estafa, fraude, falsificación, perjuicio, sabotaje etc, perjudican el bienestar de la información protegida en computadoras.

Esta delincuencia, se trata de especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando muchas veces imposible deducir como es que se realizó dicho delito.

La informática reúne características, que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo no han podido ser catalogado.

Es por ello que, la Legislación Nicaragüense ha pretendido con esta nueva legislación acercarse lo más posible a los distintos medios de protección, por lo que se debería de crear una nueva y rígida regulación especial de los Delitos Informáticos de una forma general.

El Derecho Informático, debe ser conocido por todos los seres que quieren y desean saciarse del conocimiento; es por ello, que es necesaria la enseñanza de este nuevo Derecho, esto podrá ser un logro para todas las escuelas jurídicas y las escuelas informáticas.

Existen factores que han determinado la generación de estas nuevas figuras delictivas en los Delitos Informáticos, ya que con ello viene a dar una mejor tregua a los delincuentes y personas que desean o consiguen información en banco de datos que a ellos les genera un beneficio en particular. Los fines de esta norma, conllevan a ser más capaces de conocer el mundo del Derecho Informático, su movimiento, alcance y magnitud.

En nuestro país, el Derecho Informático poco a poco tiene que ir entrando en el conocimiento de los Estudiantes de Derecho, así como también a los maestros que imparten sus clases en los salones de las facultades. Urge, que en el país se genere y/o se practique el estudio del Derecho Informático.

Primeramente, en el primer capítulo abordo de manera general los Delitos Informáticos, su definición, Características, Elementos de los Delitos Informáticos, Sujetos del Delito, Clasificación, y sus Formas de control, y los tipos de clasificación de los delitos informáticos de acuerdo al uso de la computadora como medio, como fin o por los tipos de ataques contra los sistemas de información, la sugerida por la Organización de las Naciones Unidas (ONU) y otros autores.

Luego a bordo de manera más detallada los tipos de Delitos Informáticos regulados en el nuevo Código Penal de la República de Nicaragua, mostrando la descripcion de los mismos y su penalización.

Y finalmente, se aborda sobre los Bienes Jurídicos tutelados en el nuevo Código Penal vigente de la República de Nicaragua con respecto a los Delitos Informáticos.

CAPITULO I
DELITOS INFORMÁTICOS

CAPITULO I

DELITOS INFORMÁTICOS

1.- ANTECEDENTES

Cual es la historia de los Delitos Informáticos?

Se podría decir que los Delitos Informáticos surgen antes de que existiese la Informática, tal como la concebimos hoy.

Orígenes de Internet

El 4 de Octubre de 1957 la antigua Unión Soviética puso en órbita el primer satélite artificial, llamado ***SPUTNIK****, adelantándose a los Estados Unidos de América que 2 años antes había anunciado el inicio de una carrera inter-espacial.* [1]

Un año después, el presidente ***Dwight Eisenhower*** *ordenó la creación de la* ***ADVANCED RESEARCH PROJECTS AGENCY*** *(ARPA) creado por el Departamento de Defensa de los EUA así como la* ***NASA****.*[2]

Este importante hecho marca el comienzo del uso de las comunicaciones globales.

En el año 1961 el Director del Defense Research and Engineering (DDR&E) asigna las funciones del ARPA.

Pasaron 5 años y en lo que se llamó la época de la Guerra Fría entre las más grandes potencias del mundo.

---

[1] *http://www.perantivirus.com/sosvirus/pregunta/delitoshistory.htm*
[2] *Idem*

El gobierno de los Estados Unidos encargó en Octubre de 1962 a JCR Licklider, del Massachusetts Institute of Technology (MIT) que liderase a un grupo de investigadores y científicos para emprender el proyecto, ARPA, con fines de proteccionismo bélico en la eventualidad de un conflicto mundial.[3]

Entre 1962 y 1968 se trabajó el concepto de intercambio de paquetes, desarrollado por Leonard Kleintock y su origen y uso fue meramente militar. La idea consistía en que varios paquetes de información pudiesen tomar diferentes rutas para uno o más determinados destinos, consiguiendo con ello una mejor seguridad en el trasporte de la información. [4]

Se siguieron conectando computadores rápidamente a la ***ARPANET*** *durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red.*

En Diciembre de 1970, el Network Working Group (NWG) liderado por S.Crocker acabó el protocolo ***host a host*** *inicial para ARPANET, llamado Network Control Protocol (NCP). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-1972, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones.*[5]

1991 - El ***Gopher*** *es creado por la Universidad de Minnesota. El Gopher provee al usuario de un método basado en un menú jerárquico, que es capaz de localizar información en la Internet. Esta herramienta facilita enormemente el uso de la Internet.*[6]

1992 Se funda la ***Internet Society****.*

---

[3] *http://www.perantivirus.com/sosvirus/pregunta/delitoshistory.htm*
[4] *Idem*
[5] *http://www.perantivirus.com/sosvirus/pregunta/delitoshistory.htm*
[6] *Ídem*

1993 - El European Laboratory for Particle Physics in Switzerland (CERN) libera el ***World Wide Web*** *(WWW), desarrollado por* ***Tim Berners-Lee****. El WWW usa el protocolo de transferencia de hipertexto (HTTP) y encadena hipertextos muy fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accedida en la Internet* [7]*.*

El especial desarrollo de las nuevas tecnologías, la informática y las telecomunicaciones, y especialmente el efecto sinérgico entre ambas, esta suponiendo un cambio trascendental en la sociedad. Trabajo, economía, administración y ocio son algunos de los aspectos que están variando a pasos agigantados, dirigiéndonos hacia esa sociedad cada vez más global, en la que la esfera de influencia supera nuestro entorno social mediato para constituirse en todo el planeta, sociedad a la que hemos bautizado como Sociedad de la Información. Y en ella, juega un papel determinante Internet como vehículo de transmisión e intercambio de todo tipo de información, produciéndose una sinécdoque entre la parte y el todo, Internet por Sociedad de la Información. [8]

Las redes de comunicación electrónica y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes.

Esta tendencia implica sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información.

Estos ataques pueden adoptar formas distintas, como el acceso ilegal, la difusión de programas perjudiciales y ataque por denegación de servicio. Es

---

[7] *Ídem*
[8] *Introducción de la Directiva 2000/31/CE (sic)*

posible "lanzarlos" desde cualquier lugar del mundo hacia el resto del planeta y además en cualquier momento. En el futuro podrían producirse nuevas formas de ataques inesperados.

Esta red ha permitido la globalización cultural y, en especial, de los mercados, diseñando nuevos escenarios socioeconómicos. El comercio electrónico, el acercamiento de bancos a clientes, la gestión electrónica de los recursos de las empresas, la videoconferencia, son una antesala de un nuevo concepto de relación laboral marcada por el distanciamiento del habitual puesto de trabajo, el teletrabajo.

La implantación de esta sociedad, que parece no conocer otro limite que la imaginación humana, puede incluso hacer tambalear los propios fundamentos del Estado y de la concepción actual de sistema democrático, dando paso quizá a una democracia electrónica.

Estas situaciones reflejadas no son más que simples conjeturas de lo que esta Sociedad de la Información puede traer consigo, junto al indiscutido incremento de la calidad de vida apoyado en el desarrollo tecnológico.

Pero esta extraordinaria expansión de las redes de telecomunicaciones trae aparejada, nuevas situaciones carentes hoy de regulación y sobre las que seguramente resulte precisa la intervención del Derecho.

Aun siendo expertos en nuestras propias áreas de especialización, desconocemos el funcionamiento intrínseco de Internet, ignoramos las sutilezas de la cultura digital y carecemos de bagaje tecnológico para llegar a fondo de muchos procesos y protocolos. La ignorancia nos conduce a sobredimensionar y mitificar las cosas.

Estamos ante una revolución sociocultural caracterizada por una gran dependencia tecnológica en la que no alcanzamos a unir los ámbitos

tecnológicos y jurídicos, que precisa de una armonización legislativa global frenada en parte por una férrea defensa de la identidad e intimidad, y que ofrece un escenario aparentemente anónimo y vulnerable, donde se desarrollan relaciones humanas y comerciales. Estamos en definitiva ante un terreno abonado para nuevas formas de vulneración de bienes jurídicos, un terreno abonado para la delincuencia.[9]

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información mas segura y de un espacio de libertad, seguridad y justicia, por lo que es importante abordar la temática con la mayor seriedad posible. [10]

2.- GENERALIDADES

La sociedad se sumerge cada día más en el fenómeno de la globalización, y éste se ha vuelto una característica esencial de toda sociedad, un elemento que conforma la globalización es la Tecnología Informática que tiene una enorme influencia en la vida diaria de todas las personas, tanto físicas como morales, a través de INTERNET, ya que se requiere para comunicarse, investigar asuntos importantes, llevar a cabo el proceso de comercialización, entre otras actividades que hoy en día son necesarias para el desarrollo humano.[11]

Los problemas que las innovaciones tecnológicas introducen en la sociedad, conforman una temática que origina la necesidad de la existencia de elementos típicos (descriptivos y normativos) que permitan legislar adecuadamente las acciones informáticas y telemáticas que deben ser

---

[9] *Salom Clotet, Juan. Delito Informático y su investigación <<Cuaderno de Derecho Judicial>> Consejo General del Poder Judicial, No. III, MADRID, 2006. Pag, 97.*
[10] *Comisión de las comunidades europeas, Bruselas, 19.01.2002,COM (2002) 173 final. 2002/0086 (CNS)*
[11] *http://paginas.tol.itesm.mx/Alumnos/A00961045/Delitos%20Inform%C3%A1ticos.doc*

prohibidas con precisión. Para lo cual creemos que es necesario fortalecer la conciencia jurídica centroamericana, de que este tipo de delitos es beneficioso que tengan una represión penal que tenga elementos comunes entre los diversos países, de forma tal que pueda haber una sanción eficaz aún cuando se cometan simultáneamente por medios telemáticos en distintos Estados.

Para tratar el tema de Delito Informático es conveniente delimitarlo jurídicamente en forma inicial definiéndolo como "la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software"

En nuestro país y en la mayoría de países centroamericanos existen determinadas conductas novedosas que implican una nueva criminalidad o comportamiento delictivo.

Con la expresión "criminalidad mediante computadoras se alude a todos los actos antijurídicos según la Ley vigente (o socialmente perjudiciables y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos"

Como en otros sectores del Derecho Informático, la regulación jurídica de la criminalidad informática presenta determinadas peculiaridades, debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan. En el plano de la Dogmática Jurídico-penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales, obligando a revisar los elementos constitutivos de gran parte de los tipos penales existentes.[12]

[12] *http://www.alfa-redi.org/rdi-articulo.shtml?x=343*

Se sabe que el INTERNET es un escenario virtual donde el usuario llamado también cybernauta o internauta, puede "navegar" o "surfear", términos utilizados para decir que los usuarios pueden obtener información relacionada con datos, imágenes, sonidos u otros elementos para satisfacer su curiosidad o simplemente, para aclarar su ignorancia sobre algún tema en específico, aunque para otros usuarios éste puede ser un medio para obtener ilegalmente beneficios o ventajas, es decir que estos avances son solamente utilizados para cometer delitos, dando origen a los llamados "Delitos Informáticos", que son el tema principal del presente trabajo, el cual dará a conocer algunos conceptos con la definición de delitos informáticos, tratará de explicar algunas de sus características, cómo se han clasificado para su entendimiento, y algunas formas de control, basándonos principalmente en el libro Derecho Informático de Julio Téllez Valdés. [13]

3.- CONCEPTO

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de Delito puede ser más compleja.

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta. Según el ilustre penalista CUELLO CALON, los elementos integrantes del delito son:

1. El delito es un acto humano, es una acción (acción u omisión).

2. Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

[13] *http://paginas.tol.itesm.mx/Alumnos/A00961045/Delitos%20Inform%C3%A1ticos.doc*

3. Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.

4. El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

5. La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

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 robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas Informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

En el ámbito Internacional se considera que no existe una definición propia del delito informático, sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades concretas del país de origen de los autores que lo conceptualizan.

El autor Ricardo Levene define como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.[14]

[14] *Levene, Ricardo. 2001. Delitos Informáticos, www.dtj.com.ar/publicaciones.html.*

Carlos Sarzana, indica en su obra Criminalità e tecnología,que los crímenes por computadora (otra denominación que se maneja a criterio de los expertos), comprenden "cualquier comportamiento criminògeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminògena", o como mero símbolo.[15]

Otros autores como Nidia Callegari lo definen como "aquel que se da con la ayuda de la informática o de técnicas anexas.[16]

Se podría definir el Delito Informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena.

3.1 TÍPICO

Julio Téllez Valdés en su libro de Derecho Informático, señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".[17]

---

[15] *Sarzana, Carlos citado por Ricardo Levene. 2001. Delitos Informáticos, www.drj.com.ar/publicaciones.html.*
[16] *Callegari, Nidia citado por Ricardo Levene. 2001. Delitos Informáticos, www.dtj.com.ar/publicaciones.html.*
[17] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 163.*

Es por ello, en cuanto a su tipicidad, hace referencia a los Delitos Informáticos que son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin.

3.2 ATÍPICO

Las causas de atipicidad se dan en los supuestos en los que concurren unas determinadas circunstancias que suponen la exclusión de la tipicidad de la conducta, negando con ello su inclusión dentro del tipo penal. Se da cuando en los elementos objetivos del tipo uno de ellos no encuadra en la conducta típica o simplemente no se da. Se dice que existe ausencia del tipo cuando en la Ley no se encuentra plasmada o regulada alguna prohibición de alguna conducta, acorde al principio de legalidad penal. Por ejemplo, la blasfemia no está tipificada como delito en la mayoría de los países. Aunque para muchos pueda ser una actitud reprochable, esta no será castigada por la Ley o el Estado, ya que no es una conducta recogida y penada en el código penal.[18]

Es por ello que Julio Téllez Valdés en su obra Derecho Informático plasma la atipicidad como las conductas, típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin.

4. CARACTERÍSTICAS

Los delitos informáticos por su particularidad poseen características que los diferencian de la mayoría de los delitos tradicionales ya tipificados, hace años, por los códigos y autores.

Las características de los Delitos Informáticos son:

[18] *http://es.wikipedia.org/wiki/Teor%C3%ADa_del_delito#Causas_de_atipicidad*

1. *Son conductas delictivas de cuello blanco (white collar crimes), en tanto que solo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.*
2. *Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto esta en el trabajo.*
3. *Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.*
4. *Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.*
5. *Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.*
6. *Son muchos los casos y pocas las denuncias, todo ello debido a la falta mimas de regulación jurídica a nivel internacional.*
7. *Son sumamente sofisticados y frecuentes en el ámbito familiar.*
8. *Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.*
9. *En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).*
10. *Ofrecen facilidades para su comisión a los menores de edad.*
11. *Tienden a proliferar cada vez mas, por lo que requieren una urgente regulación jurídica a nivel internacional.*[19]

[19] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 163.*

5. ELEMENTOS DE LOS DELITOS INFORMÁTICOS

Los Delitos Informáticos constan de dos tipos de elementos;

El primero el Elemento Objetivo y el segundo es el Elemento Subjetivo.

5.1 ELEMENTO OBJETIVO:

Es la acción, que afecta tanto a los componentes como a la computadora misma, viene siendo el borrado, destrucción o alteración de un sistema informático o de datos dentro de un sistema informático.[20]

5.2 ELEMENTO SUBJETIVO:

El elemento subjetivo está compuesto del dolo y la culpa. La intención de dañar el sistema o los datos de otro. Asimismo, debemos considerar a este delito como subsidiario, "ya que la acción de dañar es uno de los medios generales para la comisión de ilícitos, pero esta subsidiariedad está restringida exclusivamente a los casos en que el delito perpetrado por medio de la acción dañosa esté 'más severamente penado.[21]

En nuestro derecho, no existe como tal el delito informático, porque no está tipificado en el Código Penal, al no estar tipificado el delito informático, se acude al principio de legalidad en materia penal: no hay crimen sin Ley, no hay pena sin Ley, no existe delito ni pena por las acciones, por dolosas que sean.[22]

[20] *http://www.frcu.utn.edu.ar/deptos/depto_3/32JAIIO/sid/SID_02.pdf*
[21] *Idem*
[22] *Idem*

6. SUJETOS DEL DELITO

Los sujetos del delito son el Sujeto Activo y el Sujeto Pasivo, haciendo referencia en cuanto a los delitos informáticos.

6.1 SUJETO ACTIVO

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, 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.[23]

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los 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 controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

---

[23] *Barreda González, Nadiezhda Kruspkaya y otros. / Derecho Informático: Contenido y aplicación. León, Nic; UNAN 2002. Pagina 135.*

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de "cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.[24]

La "cifra negra" es muy alta; no es fácil descubrirlos ni sancionarlos, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad. A los sujetos que cometen este tipo de delitos no se considera delincuentes, no se los segrega, no se los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo "respetable". Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.[25]

6.2 SUJETO PASIVO

Este, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.[26]

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él, podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, debido a que muchos de los delitos son descubiertos causídicamente por el desconocimiento del modus operandi de los sujetos activos, por lo que ha sido imposible conocer

---

[24] *Barreda González, Nadiezhda Kruspkaya y otros. / Derecho Informático: Contenido y aplicación. León, Nic; UNAN 2002. Pagina 135.*
[25] *http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm*
[26] *http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm*

la verdadera magnitud de los delitos informáticos, ya que la mayor parte 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 delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra".[27]

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.[28]

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

7. CLASIFICACIÓN

***Julio Téllez Valdés**, clasifica los delitos informáticos en atención a dos criterios: como instrumento o medio, o como fin u objetivo.*

---

[27] *http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm*
[28] *Idem*

7.1 *COMO INSTRUMENTO O MEDIO*

En esta categoría tenemos a 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) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc).

d) "Robo" de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos tanto en la entrada como en la salida.

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto se le conoce en el medio como el método del "Caballo de Troya"). [29]

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de salami". [30]

i) Uso no autorizado de programas de cómputo.

---

[29] ***Método del caballo de Troya:*** *es el aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas.*

[30] ***Técnica de salami:*** *Es la desviación del destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.*

j) Insertar instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como consulta a su distribuidor.

k) Alteración en el funcionamiento de los sistemas.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención de las líneas de comunicación de datos de teleproceso.[31]

7.2 COMO FIN U OBJETIVO

En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

1. *Programación de instrucciones que producen un bloqueo total al sistema.*
2. *Destrucción de programas por cualquier método y daño a la memoria.*
3. *Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).*
4. *Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.*
5. *Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etcétera).*

7.3 TIPOS DE ATAQUES CONTRA LO SISTEMAS DE INFORMACIÓN

La expresión "sistema de información" se utiliza deliberadamente aquí en su sentido más amplio habida cuenta de la convergencia entre las redes de

---

[31] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 165*

comunicación electrónica y los distintos sistemas que conectan. A efectos de la presente propuesta, los sistemas de información cubren, pues, los ordenadores personales autónomos, las agendas electrónicas personales, los teléfonos móviles, los intranets, los extranets y, naturalmente, las redes, servidores y otras infraestructuras de Internet. [32]

En el texto de "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo"[33]*, la Comisión propuso la descripción siguiente de las amenazas contra los sistemas informáticos:*

1. ***ACCESO NO AUTORIZADO A SISTEMAS DE INFORMACIÓN:*** *Esto incluye el concepto de "**piratería informática".** La piratería consiste en tener acceso de manera no autorizada a un ordenador o a una red de ordenadores. Puede tomar distintas formas que van desde el mero uso de informaciones internas a ataques directos y la interceptación de contraseñas. Se realiza generalmente –pero no siempre– con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios Internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado.* [34]
2. ***LA PERTURBACIÓN DE LOS SISTEMAS DE INFORMACIÓN:*** *Existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos por Internet es el ataque de tipo **"Denegación de Servicio"** (DdS). Este ataque es en cierta medida similar al hecho de inundar las máquinas de fax con mensajes largos y*

[32] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 166.*
[33] *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de Regiones "Seguridad de las redes y de la información - Propuesta para un enfoque político europeo" del 6 de junio de 2001. COM (2001) 298 final.*
[34] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 165.*

repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios Internet (PSI) con mensajes generados automáticamente. [35]

Otros tipos de ataques pueden consistir en perturbar los servidores que hacen funcionar el sistema de nombres de dominio (DNS) y los ataques contra los "encaminadores".

3. ***EJECUCIÓN DE PROGRAMAS INFORMÁTICOS PERJUDICIALES QUE MODIFICAN O QUE DESTRUYEN DATOS.*** *El tipo más conocido de programa informático malintencionado es el virus. Los virus "I Love You", "Melissa" y "Kournikova" son ejemplos conocidos. Alrededor de 11% de los usuarios europeos se han visto afectados por un virus en su ordenador personal (PC). Existen otros tipos de programas informáticos perjudiciales. Algunos dañan al propio ordenador, mientras que otros utilizan el PC para atacar otros elementos de la red. Algunos programas (llamados "bombas lógicas") pueden permanecer inactivos hasta que se desencadenan por algún motivo como, por ejemplo, una fecha determinada y causan graves daños modificando o destruyendo datos. Otros programas parecen benignos, pero cuando se los lanza, desencadenan un ataque perjudicial (por eso se los llama "Caballos de Troya"). Otros programas (llamados "gusanos") no infectan otros programas como los virus, pero crean réplicas de ellos mismos, estas réplicas crean a su vez nuevas réplicas y de este modo se termina por inundar el sistema.*[36]
4. ***INTERCEPTACIÓN DE LAS COMUNICACIONES:*** *La interceptación malintencionada de comunicaciones afecta a los requisitos de*

[35] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 167.*
[36] *Idem*

confidencialidad e integridad de los usuarios. Se le denomina a menudo "sniffing" (intromisión).[37]

5. ***DECLARACIONES FALSAS:*** *Los sistemas de información ofrecen nuevas posibilidades de declaraciones falsas y de fraude. El hecho de usurpar la identidad de otra persona en Internet y de utilizarla con fines malintencionados se llama "spoofing" (modificación de los datos).* [38]

8. FORMAS DE CONTROL

Como podemos inferir, este tipo de ilícitos requieren de un necesario control, y éste, al no encontrar en la actualidad un adecuado entorno jurídico, ha tenido que manifestarse, en su función preventiva y correctivo.

8.1 PREVENTIVO

Esta se puede realizar, a través de diversas formas de carácter administrativo, normativo y técnico, de entre las que se cuentan las siguientes:

1. *Elaboración de un examen psicométrico previo al ingreso al área de sistemas en las empresas.*
2. *Introducción de cláusulas especiales, en los contratos de trabajo con el personal informática que por el tipo de labores a realizar así lo requiera.*
3. *Establecimiento de un código ético de carácter interno en las empresas.*
4. *Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.*
5. *Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.*
6. *Identificación, y en su caso segregación, del personal informática descontento.*

---

[37] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 167.*
[38] *Idem*

7. *Rotación en el uso de claves de acceso al sistema (passwords).* [39]

8.2 CORRECTIVO

Esto podrá darse en la medida en que se introduzcan un conjunto de disposiciones jurídicas específicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas ya existentes, se corte el riesgo de alterar de manera flagrante el principio de legalidad de las penas. (Nulla pena sine legem).[40]

Cabe hacer mención, que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en buen número este tipo de acciones que tanto daño causan a los intereses individuales y sociales.

El objetivo de la creación de un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia, organizada o no, incluido el terrorismo, mediante una cooperación mas estrecha entre los servicios represivos y las autoridades judiciales de los distintos Estados interesados, al uniformar las legislaciones y las normas en materia de cooperación policial y judicial penal, la Corte Penal Internacional (Estatuto de Roma) pone de relieve la necesidad de pensar cada vez mas, en una "universalización" del Derecho.[41]

---

[39] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 175.*

[40] *De acuerdo a este principio, la Ley es fuente exclusiva para establecer los delitos y las penas de tal manera que todo aquello que no está descrito en la Ley como delito no puede ser castigado. La exclusividad de la Ley como fuente de delitos y penas esta incorporado en la totalidad de las Constituciones y Códigos Penales.*

[41] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 176.*

9. TIPOS DE DELITOS REALIZADOS POR MEDIOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE NACIONES UNIDAS (ONU)

I.- FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS

1. ***MANIPULACIÓN DE LOS DATOS DE ENTRADA:*** *Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.*

   Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
2. ***MANIPULACIÓN DE PROGRAMAS:*** *Es muy difícil de descubrir y a menudo pasa inadvertida 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, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.*
3. ***MANIPULACIÓN DE LOS DATOS DE SALIDA:*** *Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones 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 equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

4. ***MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE 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 transfieren a otra.*

II.- FALSIFICACIONES INFORMÁTICAS

1. ***COMO OBJETO:*** *Cuando se alteran datos de los documentos almacenados en forma computarizada.*
2. ***COMO INSTRUMENTOS:*** *Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.*

III.- DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS

1.- SABOTAJE INFORMÁTICO: *Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con*

intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

1.1.- VIRUS: *Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse 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.*

1.2.- GUSANOS: *Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.*
En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

1.3.- BOMBA LÓGICA O CRONOLÓGICA: *Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés 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.

IV.- ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

1. ***PIRATAS INFORMÁTICOS O HACKERS:*** *El acceso se efectúa a menudo 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.*
2. ***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.[42]

9.1 OTROS AUTORES

Siempre en lo concerniente a los Delitos Informáticos, el autor Olivier Hance en su libro Leyes y Negocios en Internet, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a) ***ACCESO NO AUTORIZADO:*** *es el primer paso de cualquier delito. Se refiere a un usuario que sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente, pero decide voluntariamente mantenerse conectado.*

b) ***ACTOS DAÑINOS O CIRCULACIÓN DE MATERIAL DAÑINO:*** *una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).*

c) ***INTERCEPTACIÓN NO AUTORIZADA:*** *en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.*[43]

---

[42] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 72-174.*

[43] *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004. Pág. 168.*

9.2 OTRAS CLASIFICACIONES

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

1. ***ACCESO NO AUTORIZADO:*** *Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.*
2. ***DESTRUCCIÓN DE DATOS:*** *Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.*
3. ***INFRACCIÓN AL COPYRIGHT DE BASES DE DATOS:*** *Uso no autorizado de información almacenada en una base de datos.*
4. ***INTERCEPTACIÓN DE E-MAIL:*** *Lectura de un mensaje electrónico ajeno.*
5. ***ESTAFAS ELECTRÓNICAS:*** *A través de compras realizadas haciendo uso de la red.*
6. ***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 delitos:

1. ***ESPIONAJE:*** *Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.*
2. ***TERRORISMO:*** *Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.*
3. ***NARCOTRÁFICO:*** *Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.*

4. ***OTROS DELITOS:*** *Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.*

Cabe mencionar la distinción entre hacker, que por grandes conocimientos y habilidades en materia informática y que dicen solo buscar las "fallas de seguridad" y los Cracker, que se valen de los dispositivos o programas generados por los hackers, para cometer deliberadamente delitos.

CAPITULO II
TIPOS DE DELITOS REGULADOS EN EL NUEVO CÓDIGO PENAL

CAPITULO II

TIPOS DE DELITOS REGULADOS EN EL NUEVO CÓDIGO PENAL

En este Capitulo, hago un señalamiento de los Delitos relacionados a la informática contenido en el nuevo código penal, así como la descripción del tipo de los mismos, partiendo de la relación que existe entre el derecho penal y el derecho informático.

El derecho penal, es el conjunto de normas que determinan los delitos y las penas que el Estado impone a los delincuentes y las medidas de seguridad que él mismo establece para la prevención de la criminalidad.

En el nuevo Código Penal de la Republica de Nicaragua, se recogen, como delitos informáticos los siguientes:

1.- Arts. 192 – 195 – 199 (Apertura o interceptación ilegal de comunicaciones).
2.- Arts. 229 (Estafa).
3.- Arts. 245 (Daños)
4.- Arts. 246 (Programas destructivos)
5.- Arts. 247 (Delitos contra el derecho de autor y derechos conexos)
6.- Arts. 248 (Reproducción ilícita)
7.- Arts. 249 (Delitos contra las señales digitales)
8.- Arts. 250 (Protección de programas de computación)

Dada la gama de Delitos informáticos anteriormente, a continuación se definirá cada delito y se señalara la tipificación.

1.- APERTURA O INTERCEPTACIÓN ILEGAL DE COMUNICACIONES

La interceptación ilegal de comunicaciones representan un claro atentado contra el derecho de las personas al secreto e inviolabilidad de sus comunicaciones, demandado por la Constitución política de Nicaragua.

En el titulo III, capítulo I, articulo 192 ***Apertura o interceptación ilegal de comunicaciones;*** *castiga hasta con dos años de prisión al que al margen de la Ley abra, intercepte o por cualquier medio o un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido.*

En el titulo III, capítulo I, articulo 193 ***Sustracción, desvío o destrucción de comunicaciones;*** *castiga hasta con un año quien sin enterarse del contenido, se apodere ilegalmente, destruya o desvíe de su destino una comunicación que no le esté dirigida; y quien conociendo o presuponiendo el contenido de la comunicación realizare la conducta prevista anterior, será penado con prisión de uno a dos años.*

En el titulo III, capítulo I, articulo 194 ***Captación indebida de comunicaciones ajenas;*** *Castiga a quien hasta con dos años de prisión a quien ilegítimamente grabe las palabras o conversaciones ajenas, no destinadas al público, o el que mediante procedimientos técnicos escuche comunicaciones privadas o telefónicas que no le estén dirigidas.*

En el titulo III, capítulo I, articulo 195 ***Propalación;*** *Castiga hasta con multa de sesenta a ciento ochenta días de prisión a quien hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque a este mismo le hayan sido dirigidos.*

En el titulo III, Capitulo I, articulo 197 ***Registros prohibidos;*** *este prohíbe la comercialización de banco de datos y castiga hasta prisión de dos a cuatro años y de trescientos a quinientos días multa.*

En el titulo III, capitulo I, articulo 198 ***Acceso y uso no autorizado de información;*** *castiga hasta con tres años de prisión o su inhabilitación especial hasta por cinco años por utilizar sin autorización y el ingreso no autorizado a registros informáticos o banco de datos, esto seria lo que en esta monografía hemos llamado accesos no autorizados.*

2.- ESTAFA

Otro delito informático que claramente regula este nuevo código, es la Estafa informática contenida en el articulo 229,del libro II, del titulo VI Los delitos contra el patrimonio y el orden socio-económicos", Capitulo V ", aparece como una modalidad de la estafa tradicional, claro estableciendo la diferencia que en esta ultima se induce al error a una persona, pero en la primera (La estafa informática) lo que se requiere es una manipulación de registro o programa informático y este mismo se castiga con prisión de uno a cuatro años y noventa a trescientos días multa.

Hay que recordar los cuatro elementos de la Estafa:

1.- Engaño o presentación falsaria de una determinada realidad.
2.- Error, que sufre a consecuencia del engaño.
3.- Ánimo de lucro en el sujeto activo.
4.- Disposición patrimonial del sujeto pasivo.

Sin embargo, la "Estafa Informática" no encaja, en su dinámica comisiva, con la Estafa tradicional pues no existe realmente engaño o error,

dado que la maquina no goza de una psicología que pueda ser objeto de engaño.

Pero la nueva Estafa Informática, pivota sobre unos elementos distintos que guardan relación con la estructura clásica de la Estafa: la manipulación informática o el empleo de "artificio semejante", que equivale al engaño clásico; la transferencia no consentida, o acto de disposición de la estafa tradicional, y por supuesto, en ambos casos existe perjuicio económico, que sufre el titular de la cuenta sobre la que se produce el ataque informático.[44]

En este caso la proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.[45]

3.- DAÑOS

Un delito que podemos llamar meramente informático, en el libro II, del titulo VI, capitulo VIII articulo 245, que habla de la destrucción de registros informáticos. El objeto de protección va dirigido a la información almacenada en sistemas informáticos, protegiendo un bien jurídico como es la información.

Al pie de la letra de código penal castiga hasta dos años de prisión o multa de noventa a trescientos días. Y cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial esta se elevara hasta cinco años de prisión.

---

[44] *Urbano Castrillo "Infracciones patrimoniales por medios informáticos y contra la información, como bien económico. Cuaderno de derecho judicial. No 3, 2006. Pág. 163.*
[45] *http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo12.htm*

4.- PROGRAMAS DESTRUCTIVOS

En el libro II, del titulo VI, capítulo VIII, articulo 246 ***Uso de programas destructivos;*** *castiga a quien con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será penado con prisión de uno a tres años y multa de trescientos a quinientos días.*

La utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

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

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

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

Una variante perfeccionada de la anterior modalidad es el «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.[46]

Este artículo es de inmediata aplicación ante el caso de virus, bombas lógicas o gusanos, las tres modalidades del sabotaje informático.

5.- DELITOS CONTRA EL DERECHO DE AUTOR Y DERECHOS CONEXOS

El derecho de propiedad exclusivo se conoce como 'derecho de autor', en este sentido cualquier tipo de violación dará lugar a reparación del daño e indemnización de perjuicios.[47]

Nos podemos encontrar con la falsificación de programas informáticos, conocidos como software. Este delito es de los que puede perjudicar a mas de un bien jurídico, puesto que también afecta al patrimonio de los autores originales de los programas en cuestión, ya que la reproducción ilícita y el expendio de estas, causa merma en la economía de los propietarios de los derechos.[48]

Estas son conductas dolosas, que exigen ánimo de lucro aunque no es necesaria la producción de un perjuicio efectivo en el patrimonio del sujeto pasivo, ya que este delito es de mera actividad.

---

[46] *http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo10.htm*
[47] *http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo38.htm*
[48] *Chacon, Rina, y Gamez , Ligia, Delitos Informáticos. León, Nic; UNAN 2003. Pagina 31.*

Los derechos de creación, y los de explotación de la obra protegen tanto la preparación como la fabricación, importación, circulación o tenencia de dispositivos para cometer dicho delito.[49]

En los derechos de autor se protege la paternidad de la obra; en la explotación la reproducción, distribución, comunicación pública y la transformación inconsentidas de la obra.[50]

Esto supone entender la protección de las obras producidas o distribuidas a través de Internet (Musical, bibliográfico, cinematográfico).[51]

Cabe destacar que en nuestra legislación nicaragüense existe propiamente la Ley No 312 Ley de derechos de Autor y Derechos conexos publicada en la gaceta numero 166 del 31 de agosto de 1999 y las conclusiones publicadas en la gaceta numero 167 del 1º de Septiembre de 1999, con esta nueva implementación estos tendrán cabida en el Nuevo Código Penal de la República de Nicaragua para castigar a los delincuentes.

En el libro II, del titulo VI, capítulo IX, articulo 247 ***Ejercicio no autorizado del derecho de autor y derechos conexos;*** *castiga con prisión de seis meses a dos años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la Ley de la materia, y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los actos siguientes sin autorización escrita del titular del derecho:*

---

[49] *Urbano Castrillo "Infracciones patrimoniales por medios informaticos y contra la información, como bien económico. Cuaderno de derecho judicial. No 3, 2006. Pág. 169.*
[50] *Idem.*
[51] *Idem.*

a) La traducción, arreglo, u otra transformación de la obra;
b) La comunicación pública de una obra o fonograma por cualquier forma, medio o procedimiento, íntegra o parcialmente.
c) La retransmisión, por cualquier medio alámbrico o inalámbrico de una emisión de radiodifusión;
d) La reproducción de un mayor número de ejemplares que el establecido en el contrato;
e) Distribuir o comunicar la obra después de finalizado el contrato;
f) La atribución falsa de la autoría de una obra;
g) La realización de cualquier acto que eluda o pretenda eludir una medida tecnológica implementada por el titular del derecho para evitar la utilización no autorizada de una obra o fonograma;
h) La fabricación, importación, distribución y comercialización, o quien proporcione mecanismos, dispositivos, productos o componentes, u ofrezca servicios de instalación para evadir medidas tecnológicas enunciadas en el literal anterior;
i) La alteración, supresión de información sobre gestión de derechos; y
j) La importación, distribución, comercialización, arrendamiento o cualquier otra modalidad de distribución de obras o fonogramas cuya información sobre gestión de derechos ha sido suprimida o alterada.

6.- REPRODUCCIÓN ILÍCITA

En el libro II, del titulo VI, capítulo IX, articulo 248 ***Reproducción ilícita;*** *castiga con prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la Ley de la materia y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los siguientes actos sin autorización escrita del titular del derecho:*

a) La reproducción, total o parcial, de una obra o fonograma por cualquier medio, forma o procedimiento;
b) La distribución de ejemplares de una obra o fonograma por medio de venta, arrendamiento, préstamo público, importación, exportación o cualquier otra modalidad de distribución;
c) La fijación de la actuación de un artista intérprete o ejecutante y;
d) La fijación de una emisión protegida para su ulterior reproducción o distribución.

Este delito ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

7.- DELITOS CONTRA LAS SEÑALES DIGITALES

En el libro II, del titulo VI, capítulo IX, articulo 249 ***Delitos contra señales satelitales protegidas;*** *castiga a quien contraviniendo la Ley de la materia y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los siguientes actos sin autorización escrita del titular del derecho:*

1.- La retransmisión o distribución al público de una señal portadora de programas, sea por medios alámbricos o inalámbricos u otro medio o procedimiento similar.
2.- La decodificación de una señal codificada portadora de programas;
3.- La fijación o reproducción de las emisiones;
4.- La fabricación, ensamblaje, modificación, importación, exportación, venta, instalación, mantenimiento, arrendamiento o cualquier otra forma de

distribución o comercialización de dispositivos o sistemas que sirvan para decodificar una señal codificada portadora de programas.
5.- El que incurra en cualquiera de las conductas anteriormente señaladas, será sancionado con prisión de uno a tres años o de trescientos a quinientos días multa e inhabilitación especial por el mismo período para ejercer el cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva.

En si, estos delitos de señales satelitales es que funcionan o se pueden transmitir por cable coaxil, este mismo no es energía eléctrica. Sino, se trata de señales digitales, obtenidas de satélites, que se redistribuyen por una red de cable coaxil, a particulares que se encuentran abonados por la empresa distribuidora de Internet.

Lo que se puede interpretar en este moderno mecanismo de comunicación es una "cosa" o una "energía" o una "fuerza natural" es pura interpretación analógica, lo que no es admisible en derecho penal.

La transmisión por cable coaxil es, en síntesis, un servicio del que no resulta desapoderado el sujeto pasivo, aún concediendo que ello le cause perjuicio, como servicio no cobrado (no pierde algo que posee, sino que deja de ganar por la administración de lo que posee).

Debo señalar que puede resultar escandaloso considerar atípica la conducta de quien se apropia indebidamente de la señal que provee el servicio de Internet, más lo cierto es que la legislación no avanza a la velocidad de la tecnología, dejando fuera del alcance del derecho situaciones como la presente.

8.- PROTECCIÓN DE PROGRAMAS DE COMPUTACIÓN

En el libro II, del titulo VI, capítulo IX, articulo 250 ***Protección de programas de computación:*** *castiga con trescientos a quinientos días multa o prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la Ley de la materia:*

1.- Fabrique
2.- Distribuya o
3.- Venda mecanismos o sistemas que permitan o faciliten la supresión no autorizada de dispositivos técnicos que se hayan utilizado para evitar la reproducción de programas de computación.

CAPITULO III
BIENES JURÍDICOS TUTELADOS

CAPITULO III

BIENES JURÍDICOS TUTELADOS

Introduciéndonos mas en el ámbito de lo jurídico nos corresponde explicar ahora algunos bienes jurídicos tutelados del derecho penal y su correspondiente aplicación dentro de los delitos informáticos que pretenden proteger a la información como base esencial de las actividades a través de Internet.

El código penal consagra como delitos una lista de conductas por ser estas contrarias a un valor social; dicho valor social, es lo que dentro de la dogmática jurídica se conoce como Bien jurídico. Ejemplo, En el delito de homicidio la conducta que se prohíbe es "matar a otro" y el correspondiente Bien jurídico que se protege es la vida.

Una primera tesis considera que los delitos que se cometan a través de Internet se pueden encuadrar dentro de los delitos comunes del Código Penal, como el hurto, estafa o daño en bien ajeno, por lo que no consideran a la información como un Bien jurídico.

Otra tesis considera que se debe proteger la información por si misma, y que deben existir delitos exclusivamente para lograr la protección de esta sin importar su posterior utilización. Una tesis intermedia plantea que la información es un Bien jurídico intermedio, me inclino por esta tesis ecléctica que se explica a continuación.

LA INFORMACIÓN COMO BIEN JURÍDICO INTERMEDIO.

Un bien jurídico intermedio es aquel que pretende sobreproteger un valor individual a través de la protección de un bien jurídico colectivo. Tal es lo que ocurre con los delitos contra el medio ambiente que protegen el ambiente sano y que finalmente sobreprotegen la vida. Es decir el bien jurídico final e individual es la vida y el bien jurídico intermedio y colectivo es el medio ambiente.

1.- DERECHO A LA PRIVACIDAD E INTIMIDAD

La privacidad puede ser definida como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial.

Aunque privacy deriva del latín privatus, privacidad se ha incorporado a nuestra lengua en los últimos años a través del inglés, por lo cual el término es rechazado por algunos como un anglicismo, alegando que el término correcto es intimidad, y en cambio es aceptado por otros como un préstamo lingüístico válido.

Según el Diccionario de la lengua española de la Real Academia Española - DRAE, privacidad se define como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" e intimidad se define como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

El desarrollo de la Sociedad de la Información y la expansión de la Informática y de las Telecomunicaciones plantea nuevas amenazas para la

privacidad que han de ser afrontadas desde diversos puntos de vista: social, cultural, legal, tecnológico.

Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.[52]

El derecho a la intimidad es aquel derecho que garantiza un ámbito privado reservado a la propia persona y del que quedan excluidos los demás, salvo, desde luego, que el titular del derecho desee compartir esa zona de privacidad con otros semejantes.

El derecho a la intimidad es personalísimo y toda persona lo tiene por el hecho de serlo. Ella misma es la que debe determinar cuándo y hasta qué medida quiere exteriorizarse y ponerse en contacto con la sociedad.

Los sistemas de información cubren, pues, los ordenadores personales autónomos, las agendas electrónicas personales, los teléfonos móviles, los intranets, los extranets y, naturalmente, las redes, servidores y otras infraestructuras de Internet, es por ello que este derecho a la privacidad es muy vulnerable ya que existen muchas maneras a como observamos en los capítulos anteriores, dichos delitos se pueden efectuar o llevar a cabo maniobras que violenta la privacidad de los sistemas de información, que al

[52] *http://es.wikipedia.org/wiki/Seguridad_en_Internet*

mismo tiempo se encuentran protegidos por ser de mucha importancia, estas pueden ser maquinas conectadas a redes publicas, como por ejemplo, las empresas privadas y publicas, la banca y los hogares particulares. Hasta el mismo estado puede ser vulnerable siendo violentado el derecho a su defensa y la privacidad de la información.

Nos encontramos ante la presencia de dos derechos fundamentales, consagrados tanto por nuestra carta magna, como en instrumentos internacionales debidamente ratificados por Nicaragua.

El derecho a la intimidad (privacidad) en la legislación y en la jurisprudencia

Declaraciones Universales:

El Artículo 12 de la "Declaración Universal de los Derechos Humanos" adoptada por la Asamblea General de Naciones Unidas establece que el derecho a la vida privada es un derecho humano:

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques."

El Artículo 17 del "Pacto Internacional de Derechos Civiles y Políticos" adoptado por la Asamblea General de Naciones Unidas, consagra, al respecto, lo siguiente:

"1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a

su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques."[53]

Legislación europea:

La Directiva Europea 95/46 CE de 24 de Octubre del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Legislación nacional en los países Europeos:
España:

El Art. 18 de la "Constitución española de 1978" establece:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."[54]

[53] *http://es.wikipedia.org/wiki/Privacidad*
[54] *http://es.wikipedia.org/wiki/Privacidad*

Legislación de los países americanos:

Costa Rica:

El Artículo 11 de la "Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica", establece que:

Protección de la honra y dignidad:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. [55]

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques."

Jurisprudencia Europea

El Tribunal europeo de Derechos Humanos (TEDH) ha determinado que: "El concepto de vida privada alcanza a la integridad física y moral de una persona, y en consecuencia incluye su vida sexual".[56]

Nuestra constitución política *es clara en el arto 26, numeral 2 que textualmente dice así:*

Toda persona tiene derecho:

*1.- A la inviolabilidad de su domicilio****, su correspondencia y sus***

[55] *Idem*
[56] *http://es.wikipedia.org/wiki/Privacidad*

comunicaciones de todo tipo.[57]

Cuando hablamos de correspondencia estamos aludiendo a su privacidad en intimidad de información que a su vez es protegida por código penal de Nicaragua, en el titulo III, capítulo I, articulo 192 Apertura o interceptación ilegal de comunicaciones; lo cual se castiga con dos años de prisión al que al margen de la Ley abra, intercepte o por cualquier medio o un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido.[58]

2.-DERECHO A LA PROPIEDAD

La propiedad ha sido definida de diferentes maneras por los distintos autores, así encontraremos entre las diferentes definiciones, la de César Ramos que la citamos como la principal:

La propiedad ha sido definida de diferentes maneras por los distintos autores, así encontraremos entre las diferentes definiciones, la de César Ramos que la citamos como la principal:

"La propiedad (dominio): Es el derecho real mas amplio contenido, ya que comprende todas las facultades que el titular puede ejercer sobre las cosas y es un derecho autónomo por cuanto no depende de ningún otro. Es el dominio más general que puede ejercer sobre las cosas".[59]

Así como ***César Ramos*** *existen otros autores de definen a la propiedad como:*

1.- La propiedad como una facultad que corresponde a una persona llamada

---

[57] *Constitución política de la República de Nicaragua, Managua, Nicaragua. HISPAMER, IMPRESIONES HELIOS S.A. Septiembre 2007. Articulo 26, Num. 2*
[58] *http://www.asamblea.gob.ni/opciones/constituciones/Codigo%20Penal.pdf*
[59] *http://es.wikipedia.org/wiki/Privacidad*

propietario, de obtener directamente de una cosa determinada, toda la utilidad jurídica que esa cosa es susceptible de proporcionar".[60]

2.- La propiedad es el derecho de obtener de un objetivo toda la satisfacción que éste pueda proporcionar".[61]

3.- La propiedad es definida por Acarrias, como aquello "en virtud" de lo cual las ventajas que pueden procurar una cosa corporal son atribuidas totalmente a una persona".[62]

4.- La propiedad Girard la concibe como el derecho real por excelencia, el mas conocido y antiguo de todos los derechos reales o el dominio completo o exclusivo que ejerce una persona sobre una cosa corporal (plena in res protesta)".[63]

Finalmente, podrimos definir la PROPIEDAD como el derecho real de usar, gozar y disponer de las cosas, de las cuales se es propietario, sujeto a las restricciones impuestas por la Ley y defendible por acción reivindicatoria.[64]

Dentro de estos delitos podemos clasificar todo aquel delito informático que cause daño, una modificación, una alteración a un programa, sistema de redes o equipo de cómputo, integrado o accesorio. Como ejemplo, tenemos el sabotaje informático, el cual se puede llevar a cabo mediante innumerables técnicas, entre las cuales se encuentran los virus, bombas lógicas, gusanos, que destruyen de manera inmediata o paulatinamente, programas y datos almacenados en un equipo de computo, causando perjuicios económicos a los

[60] *http://es.wikipedia.org/wiki/Privacidad*
[61] *Idem*
[62] *Idem*
[63] *Idem*
[64] *Idem*

propietarios de las maquinas, sistemas o de la información.[65]

Por lo tanto podríamos decir que nuestro código penal protege el derecho propiedad sobre la información y sobre los elementos físicos, materiales de un sistema informático, en el caso de los delitos de Daños.

3.- PROPIEDAD INTELECTUAL

Como hemos podido ver con el avance desmedido de la tecnología digital a este fenómeno de la globalización, no ha dejado de ser parte lo referente a la protección de la propiedad intelectual.

Todo esto es como consecuencia de la misma sociedad de la información en donde con la revolucionaria era digital, el riesgo de plagio es mas evidente en cuanto a las obras protegidas, teniendo como fin único garantizar un régimen efectivo de protección de los derecho de propiedad intelectual.[66]

La propiedad intelectual, desde el punto de vista de la tradición continental europea y de buena parte de los países latinoamericanos, supone el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano.[67]

En los términos de la Declaración Mundial sobre la Propiedad Intelectual (votada por la Comisión Asesora de las políticas de la Organización Mundial de la Propiedad Intelectual (OMPI), el 26 de junio del año 2000, es entendida similarmente como "cualquier propiedad que, de común acuerdo, se considere de naturaleza intelectual y merecedora de protección, incluidas las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones

---

[65] *Chacon, Rina, y Gamez , Ligia, Delitos Informáticos. León, Nic; UNAN 2003. Pagina 32.*
[66] *Barreda Gonzales, Nadiezhda Krupskaya y otro / Derecho Informático: contenido y aplicación.- León, Nic,: UNAN, 2002. Pág. 77.*
[67] *http://es.wikipedia.org/wiki/Propiedad_intelectual*

geográficas.[68]

Existe además una corriente, especialmente la que proviene del movimiento de Software Libre, que considera que el término "Propiedad Intelectual" es engañoso y reúne bajo un mismo concepto diferentes regímenes jurídicos no equiparables entre sí, como las patentes, el derecho de autor, las marcas, las denominaciones de origen, entre otros.[69]

En este bien jurídico protegido nos podemos encontrar con la falsificación de programas informáticos, conocidos como software.

Este delito es de los que puede perjudicar mas de un bien jurídico, puesto que también afecta el patrimonio de los autores originales de los programas en cuestión, ya que la reproducción ilícita y el expendio de éstas, causa merma en la economía de los propietarios de los derechos.[70]

Es muy importante mencionar que nuestra Ley de derecho de autor y derechos conexos se define como: un conjunto de instrucciones expresadas mediante palabras, códigos, gráficos, diseños o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura autorizada, es capaz de hacer que un ordenador, un aparato eléctrico similar, sea capaz de elaborar informaciones, ejercite determinada tarea u obtenga determinado resultado. También forma parte del programa, su documentación técnica y sus manuales de uso.[71]

Muchísimas empresas, personas jurídicas y naturales, tienen sistemas informáticos que en su mayoría funciona a base de programas (Software) piratas. Y no es el único ejemplo, la música que el noventa y cinco por ciento de la población compra, es pirateada. Bien sea a partir de un disco original, usando computadoras o la tecnología necesaria, o bien puede ser pirateada a

---

[68] *Ídem*
[69] *Ídem*
[70] *Chacon, Rina, y Gamez , Ligia, Delitos Informáticos. León, Nic; UNAN 2003. Pagina 31.*
[71] *Ley No. 312, aprobada el 26 de agosto de 1999. Publicada en la gaceta No. 166 y 167 del 31 de agosto y 1 de septiembre de 1999.*

través de internet y luego quemada a un Cd que luego se compra.

Es por ello que con esta nuevo código penal esta al alcance de poder llevar a los que cometen este tipo de delitos que además afectan económicamente al propietario intelectual, y estos delitos pueden ser:

1.- La traducción, el arreglo y/o la transformación de la obra;

2.- La comunicación pública de una obra o fonograma por cualquier forma, medio o procedimiento, íntegra o parcialmente.,

3.-La retransmisión, por cualquier medio alámbrico o inalámbrico de una emisión de radiodifusión;

4.- La reproducción de un mayor número de ejemplares que el establecido en el contrato;

5.- Distribuir o comunicar la obra después de finalizado el contrato;

6.- La atribución falsa de la autoría de una obra;

7.-La realización de cualquier acto que eluda o pretenda eludir una medida tecnológica implementada por el titular del derecho para evitar la utilización no autorizada de una obra o fonograma;

8.- La fabricación, importación, distribución y comercialización, proporcionamiento de mecanismos, dispositivos, productos o componentes, u ofrecimientos de servicios de instalación para evadir medidas tecnológicas enunciadas en el literal anterior;

4.- DERECHO AL PATRIMONIO

La protección del patrimonio de los ciudadanos forma parte de los bienes jurídicos tutelados en la constitución política de Nicaragua y el nuevo código penal de la república de Nicaragua, creando estabilidad y confianza en el sistema económico y financiero del país y en las instituciones publicas del estado.

Podemos clasificar dentro de estos delitos a los que perjudican económicamente a un individuo o a una empresa, como es el caso de la estafa informática, el fraude informático y todo aquel ilícito que involucre los elementos tecnológicos para mermar o perjudicar el patrimonio de una persona jurídica o natural.

El derecho al patrimonio lo tiene aquella persona que posee facultades exclusivas para la realización, autorización o prohibición a terceros la realización de cualquiera de los actos de explotación de las obras.

El patrimonio puede ser afectado por los delitos informáticos en las bases de datos informáticas de las instituciones de los registros públicos de patrimonio o propiedad, estas pueden ser instituciones públicas o privadas.

5.- AFECTACIONES A LA FE PÚBLICA

El manejo irregular e ilegal de los datos consignados en documentos electrónicos, conllevan a una alta trascendencia social, con respecto al patrimonio y/o seguridad publica.

Un ejemplo de afectación publica sería que al guardar el contenido de una declaración judicial en un soporte electrónico como es el registro de datos en un disco magnético o duro, creamos un documento público en soporte electrónico, el cual su original es el que está contenido en él y no la copia que se le ordena al computador imprimir, lo que a su vez me permite concluir que dicho contenido puede ser vulnerado y por ende atentar la fe pública.

Además existen una variedad de delitos que pueden afectar la fe pública, como son:

1.-Falsificación de moneda, billetes de banco, títulos al portador y documentos de crédito que pueden ser realizados con artefactos tecnológicos de punta.
2.- Falsificación de sellos, timbres y marcas, este se pueden realizar con escáneres, para imprimirse en títulos que pueden para consumar el delito.
3.-Falsificación de documentos, lo cual trae consigo delitos de orden económico.
4.- Fraudes al comercio y a la industria, este fraude puede consumarse con la falsificación de documentos y copias ilegitimas de documentos que contienen un valor económico.
5.- Giro fraudulento de cheques.

Este Bien, es uno de los que a la postre tienen una mayor relevancia jurídica, sin descartar claro, la que tiene por si sola, los demás bienes jurídicos tutelados en el ordenamiento jurídico de Nicaragua.

6.- SEGURIDAD DEL ESTADO

Seguridad es la condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.[72]

La seguridad del estado es otro bien jurídico protegido, los delitos informáticos trascienden hasta el Estado.

[72] *http://www.xombra.com/go_articulo.php?articulo=16*

Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

1.- Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
2.-Confidencialidad: La información sólo debe ser legible para los autorizados.
3.- Disponibilidad: Debe estar disponible cuando se necesita.

4.- Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.[73]

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea comprometida.

Los delitos informáticos pueden trascender con acceso indebido a un sistema, logrando burlar a los sistemas de seguridad nacional del estado, incluso este mismo puede ser usado como sabotaje o daños a medios informáticos del mismo.

[73] *http://apuntes.danielcastelao.org/julia/IAIX/Tema_3/SEGURIDAD%20E%20INTEGRIDAD%20DE%20LA%20INFORMACION.pdf*

Existen también las posibilidades de burlar la seguridad interior del estado, como la posesión de equipos dentro del estado nacional, que pueden ser usados como sistema de vigilancia internacional, poniendo en riesgo la seguridad interna del estado.[74]

Este bien jurídico es muy importante, vale por si mismo y el mismo estado de Nicaragua ha logrado crear un código relevante en cuestión de ataques informáticos que pueden darse dentro de la red que posee nuestra nación.[75]

Esto también puede darse por medio de un sinnúmero de servidores públicos y privados los cuales pueden servir para el espionaje informático, que incluye la obtención, difusión y revelación de información, muy valiosa para el Estado de Nicaragua. Estos directamente afectan la seguridad del Estado y a la defensa nacional.

[74] *http://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml*
[75] *Idem*

CONCLUSIONES

La distribución en el articulado del nuevo Código Penal de la Republica de Nicaragua, sobre la nueva figura jurídica de imputación del Delito Informático se encuentra basada no solo en la protección de la información, sino que también en la protección de la libertad, integridad física y/o sexual de las personas.

Con respecto a la protección de la información, los Delitos Informáticos, también se encuentran revestidos en los delitos contra la vida privada, en defraudaciones como la estafa ocasionando daños y perjuicios que se encuentran tipificados en el Código Penal de la Republica de Nicaragua.

Los delitos informáticos también, afectan a otro grupo de población, refiriendo a los delitos contra el Derecho de Autor y Derechos Conexos, afectando el Derecho de libre competencia y a los consumidores, dentro de esta figura delictiva se encuentra los delitos contra el sistema bancario y financiero. Los delitos de acceso a la información se dan en el contexto de la divulgación de información pública.

Todos estos delitos informáticos como vemos, pueden afectar al ser humano su derecho a no ser violada su integridad, el derecho que tienen las instituciones a estar protegidas por la legislación al uso debido de la información en medios electrónicos, banco de datos, instrucción con llaves electrónicas al ingresar a bodegas con códigos digitalizados o con llaves electrónicas.

En esta delincuencia, se trata de especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando muchas veces imposible deducir como es que se realizó dicho delito.

La informática reúne características, que la convierten en un medio idóneo para la comisión de nuevas tipos de delitos que en gran parte del mundo no han podido ser catalogado.

Es por ello que, la legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, por lo que se debería de crear una nueva y rígida regulación especial de los Delitos Informáticos de una forma general.

La realidad es que, la computadora no es la que atenta contra el hombre y los bienes protegidos por la legislación, sino que es el mismo hombre el que encontró una nueva herramienta, quizás la mas poderosa hasta el momento para delinquir.

La humanidad no esta frente al peligro de la informática, sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Ha habido soluciones posibles por las consecuencias que trae consigo el Delito Informático, como es la regulación que en algunos países han implementado Leyes especiales para enfrentar estos tipos de delitos. Como ejemplo tenemos las legislaciones siguientes: Alemania, Austria, Chile, China, España, Estados Unidos, Francia, Holanda, Inglaterra y otras.
La Organización de Naciones Unidas (ONU) ha reconocido los tipos de Delitos Informáticos como:
1.- Fraudes cometidos mediante manipulación de computadoras
2.- Manipulación de los datos de entrada
3.- Daños o modificaciones de programas o datos computarizados

Adicionalmente a estos tipos de Delitos reconocidos, el XV congreso internacional de derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información como son:

Fraude en el campo de la información, falsificación en materia informática, sabotaje informático y daños a datos computarizados o programas informáticos, acceso no autorizado, intercepción sin autorización, reproducción no autorizada de un programa informático protegido, espionaje informático, uso no autorizado de una computadora, trafico de claves informáticas obtenidas por medio de ilícito y la distribución de virus o programas delictivos.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes.
Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

La importancia de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mas allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Por tanto la responsabilidad de los legisladores y la aplicación del mismo Codigo Penal no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los Delitos Informáticos.

En Nicaragua, con la nueva aprobación de este código, puede que se complemente con otras Leyes ya aprobadas como la Ley No 312 Ley de derechos de Autor y Derechos conexos, Ley de acceso a la información pública Ley no. 621 etc., garantizando la privacidad y confidencialidad de los datos que se encuentran en los ordenadores.

Es necesario que, así como en otros trabajos monográficos se pide que se legisle y se cree un marco legal que traiga aparejado consigo un regulación rígida tipificando el Delito Informático en la norma legal, se garantice la correcta aplicación.

Pero es necesario que el gobierno mismo, proporcione los medios técnicos dedicados a la actividad investigadora de estos delitos, creando órganos especializados en los cuerpos judiciales preparados en la materia para ejecutarlo, la creación de grupos específicos para la persecución de este tipo de delitos, trabajando conjuntamente estos mismos a la practica judicial y a la creación de jurisprudencia en esta materia.

Y por ultimo hacerle un llamado a nuestra universidad que ofrece la carrera de Derecho e Informática y/o telemática, que aporte a la modernización de las nuevas tecnologías y de las ciencias que a como sabemos esta ligada el Derecho Informatico a la carrera de Derecho, esto como parte de la formación de profesionales modernos de educación solida y de alta calidad.

BIBLIOGRAFÍA

1. *Barreda Gonzáles, Nadiezhda Kruspkaya y otros. / Derecho Informático: Contenido y aplicación. León, Nic; UNAN 2002.*

2. *Castellón Barreto Ernesto y Hernández León Luis / Apuntes de derecho penal. Nic: Editorial universitaria, 1998.*

3. *Diccionario nuevo mundo lengua española – Ediciones nuevo mundo – Dirección Gustavo a. Dos Santos. – España 1999.*

4. *Chacon Pantoja Rina María y Gámez valle Ligia María, Los delitos informáticos como bien jurídico protegido en materia penal. . – León Nic. Unan- León, 2003.*

5. *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de Regiones "Seguridad de las redes y de la información - Propuesta para un enfoque político europeo" del 6 de junio de 2001. COM (2001) 298 final.*

6. *Comisión de las comunidades europeas, Bruselas, 19.01.2002,COM (2002) 173 final. 2002/0086 (CNS)*

7. *Constitución Política de la Republica de Nicaragua – Managua, Nicaragua. Hispamer Impresiones Helios, S.A. Septiembre 2007.*

8. *Código penal de la República de Nicaragua, la "Gaceta diario Oficial" No 83, Ley # 641. 5 de mayo de 2008.*

9. *Ley de Derecho de Autor y Derechos Conexos, aprobada el 26 de agosto de 1999. Publicada en la gaceta No. 166 y 167 del 31 de agosto y 1 de septiembre de 1999.*

10. *Salom Clotet, Juan. Delito Informático y su investigación <<Cuaderno de Derecho Judicial>> Consejo General del Poder Judicial, No. III, MADRID, 2006. Pág, 97.*

11. *Téllez Valdés, Julio / Derecho Informático.- Tercera Edición, McGraw-Hill Interamericana Editores S.A, México, 2004.*

12. *Urbano Castrillo "Infracciones patrimoniales por medios informáticos y contra la información, como bien económico. Cuaderno de derecho judicial. No 3, 2006. Pág. 163.*

Internet

1.- http://www.perantivirus.com/sosvirus/pregunta/delitoshistory.htm

2.http://paginas.tol.itesm.mx/Alumnos/A00961045/Delitos%20Inform%C3%A1ticos.doc

3.- http://www.alfa-redi.org/rdi-articulo.shtml?x=343

4.http://paginas.tol.itesm.mx/Alumnos/A00961045/Delitos%20Inform%C3%A1ticos.doc

5.- www.dtj.com.ar/publicaciones.html.

6.http://es.wikipedia.org/wiki/Teor%C3%ADa_del_delito#Causas_de_atipicidad

7.- http://www.frcu.utn.edu.ar/deptos/depto_3/32JAIIO/sid/SID_02.pdf

8.- http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

9.http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo12.htm

10.http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo10.htm

11.http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo38.htm

12.- http://es.wikipedia.org/wiki/Seguridad_en_Internet

13.- http://es.wikipedia.org/wiki/Privacidad

14.- http://www.asamblea.gob.ni/opciones/constituciones/Codigo%20Penal.pdf

15.- http://es.wikipedia.org/wiki/Propiedad_intelectual

16.- http://www.xombra.com/go_articulo.php?articulo=16

17.http://apuntes.danielcastelao.org/julia/IAIX/Tema_3/SEGURIDAD%20E%20INTEGRIDAD%20DE%20LA%20INFORMACION.pdf

18.- http://www.delitosinformaticos.com/estafas/delitosvenezuela.shtml

19.-http://archivo.elnuevodiario.com.ni/2000/febrero/26-febrero-2000/nacional/nacional10.html

20.-http://archivo.elnuevodiario.com.ni/2002/febrero/20-febrero-2002/nacional/nacional13.html

21.http://www.laprensa.com.ni/archivo/2000/octubre/23/nacionales/nacionales-20001023-06.html

22.- http://impreso.elnuevodiario.com.ni/2008/01/26/nacionales/68816

23.- http://impreso.elnuevodiario.com.ni/2009/03/28/nacionales/98537

24.- http://www.capitalnews.es/articulo.php?n=090508061934

25.-http://www.europapress.es/cantabria/noticia-dos-imputados-estafar-mas-3000-euros-internet-20090507135317.html

ANEXOS

TÍTULO III

DELITOS CONTRA LA VIDA PRIVADA Y LA INVIOLABILIDAD DEL DOMICILIO

CAPÍTULO I

DELITOS CONTRA LA VIDA PRIVADA

Art. 192. Apertura o interceptación ilegal de comunicaciones
Quien ilegítimamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático**,** electrónico o de otra naturaleza que no le esté dirigido, será penado con prisión de seis meses a dos años.
Si además difundiera o revelara el contenido de las comunicaciones señaladas en el párrafo anterior, se impondrá prisión de uno a tres años.

Art. 193. Sustracción, desvío o destrucción de comunicaciones
Quien sin enterarse de su contenido, se apodere ilegalmente, destruya o desvíe de su destino una comunicación que no le esté dirigida, será penado con prisión de seis meses a un año.
Quien conociendo o presuponiendo el contenido de la comunicación realizare la conducta prevista en el párrafo anterior, será penado con prisión de uno a dos años.

Art. 194. Captación indebida de comunicaciones ajenas
Quien ilegítimamente grabe las palabras o conversaciones ajenas, no destinadas al público, o el que mediante procedimientos técnicos escuche comunicaciones privadas o telefónicas que no le estén dirigidas, será penado con prisión de uno a dos años.

Art. 195. Propalación
Quien hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque le hayan sido dirigidos, será penado con multa de sesenta a ciento ochenta días.

Art. 196. Violación de secreto profesional
Quien por razón de su investidura, oficio, cargo, empleo, profesión o arte, tenga noticia de un secreto cuya divulgación pueda causar daño, y lo revele sin justificación legítima, será penado con prisión de uno a tres años e inhabilitación especial de dos a cinco años para ejercer el cargo, profesión u oficio de que se trate**.**

Art. 197. Registros prohibidos
El que sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas, será penado con prisión de dos a cuatro años y de trescientos a quinientos días multa.
Asamblea Nacional. Proyecto de Ley No. 641, Código Penal, aprobado el 13 de noviembre 2007

Art. 198. Acceso y uso no autorizado de información
Quien, sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos, será penado con prisión de uno a dos años, y de doscientos a quinientos días.

DE LAS DEFRAUDACIONES

Art. 229. Estafa
Quien con el propósito de obtener un provecho ilícito, para sí o para un tercero, mediante ardid o engaño, induzca o mantenga en error a otra persona para que realice una disposición total o parcial sobre el patrimonio propio o ajeno, siempre que el valor del perjuicio patrimonial exceda la suma equivalente a dos salarios mínimos mensuales del sector industrial, será penado con prisión de uno a cuatro años y noventa a trescientos días multa.
La misma pena se impondrá a quien con el propósito de obtener un provecho ilícito, consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante la manipulación de registros informáticos o programas de computación o el uso de otro artificio semejante.

Art. 230. Estafa agravada
La estafa será sancionada con prisión de tres a seis años y trescientos a quinientos días multa, en los casos siguientes:
a) Cuando su objeto lo constituyan viviendas o terrenos destinados a la construcción de aquellas u otros bienes de reconocida utilidad social;
b) Cuando se cometa con abuso de las relaciones personales existentes entre la víctima y el estafador, o éste aproveche su credibilidad empresarial o profesional;
c) Cuando recaiga sobre bienes que integren el patrimonio histórico, cultural o científico de la nación.
d) Cuando se realice por apoderado o administrador de una empresa que obtenga, total o parcialmente sus recursos del ahorro público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya obtenido sus recursos total o parcialmente del ahorro del público;
e) Cuando el valor de lo estafado y la entidad del perjuicio, coloque a la víctima o a su familia en un grave deterioro de su nivel de vida.
f) Cuando se cometa valiéndose de tarjeta de crédito o débito propia o ajena, o con abuso de firma en blanco, o,
g) Cuando se realice mediante cheque, pagaré, letra de cambio en blanco o negocio cambiario ficticio.

CAPÍTULO VIII

DE LOS DAÑOS

Art. 243. Daño
Quien destruya, inutilice, haga desaparecer o de cualquier modo dañe un bien mueble o inmueble, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado, será sancionado con prisión de seis meses a dos años o multa de noventa a trescientos días o trabajo en beneficio de la comunidad de cuarenta y cinco a doscientos días de dos horas diarias, atendida la condición económica de la víctima y la cuantía del daño, si éste excediera de dos salarios mínimos mensuales del sector industrial.

Art. 244. Daño agravado
Se impondrá prisión de dos a tres años cuando el daño:
a) Se ejecute para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
b) Se cause en archivos, registros, bibliotecas, museos u otras cosas de valor científico, artístico, cultural, histórico o religioso; en bienes de uso público, signos conmemorativos o monumentos, tumbas y demás construcciones de los cementerios;

c) Recaiga sobre medios o vías de comunicación o de tránsito, sobre puentes o canales, sobre plantas de producción o conductos de agua, de electricidad o de sustancias energéticas;
d) Se ejecute con violencia en las personas o con intimidación;
e) Deje a la víctima en grave situación económica;
f) Recaiga sobre obras, establecimientos o instalaciones militares o policiales, medios de transporte o de transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio del Ejército de Nicaragua o de la Policía Nacional;

g) Produzca infección o contagio en plantas o animales;
h) Se perpetre por tres o más personas, o,
i) Se ejecute empleando medios, procedimientos o sustancias nocivas para la salud o el ambiente.
Si el daño se produce sobre vivienda o casa de habitación, la pena será de tres a cinco años de prisión.

Art. 245. Destrucción de registros informáticos
Quien destruya, borre o de cualquier modo inutilice registros informáticos, será penado con prisión de uno a dos años o multa de noventa a trescientos días. La pena se elevará de tres a cinco años, cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial.

Art. 246. Uso de programas destructivos
Quien, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será penado con prisión de uno a tres años y multa de trescientos a quinientos días.

CAPÍTULO IX

DELITOS CONTRA EL DERECHO DE AUTOR Y DERECHOS CONEXOS

Art. 247. Ejercicio no autorizado del derecho de autor y derechos conexos
Será sancionado con noventa a ciento cincuenta días multa o prisión de seis meses a dos años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la ley de la materia, y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los actos siguientes sin autorización escrita del titular del derecho:
a) La traducción, arreglo, u otra transformación de la obra;
b) La comunicación pública de una obra o fonograma por cualquier forma, medio o procedimiento, íntegra o parcialmente.
c) La retransmisión, por cualquier medio alámbrico o inalámbrico de una emisión de radiodifusión;
d) La reproducción de un mayor número de ejemplares que el establecido en el contrato;
e) Distribuir o comunicar la obra después de finalizado el contrato;
f) La atribución falsa de la autoría de una obra;
g) La realización de cualquier acto que eluda o pretenda eludir una medida tecnológica implementada por el titular del derecho para evitar la utilización no autorizada de una obra o fonograma;
h) La fabricación, importación, distribución y comercialización, o quien proporcione mecanismos, dispositivos, productos o componentes, u ofrezca servicios de instalación para evadir medidas tecnológicas enunciadas en el literal anterior;
i) La alteración, supresión de información sobre gestión de derechos; y

j) La importación, distribución, comercialización, arrendamiento o cualquier otra modalidad de distribución de obras o fonogramas cuya información sobre gestión de derechos ha sido suprimida o alterada.

Art. 248. Reproducción ilícita
Será sancionado con trescientos a quinientos días multa o prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la Ley de la materia y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los siguientes actos sin autorización escrita del titular del derecho:
a) La reproducción, total o parcial, de una obra o fonograma por cualquier medio, forma o procedimiento;
b) La distribución de ejemplares de una obra o fonograma por medio de venta, arrendamiento, préstamo público, importación, exportación o cualquier otra modalidad de distribución;
c) La fijación de la actuación de un artista intérprete o ejecutante y;
d) La fijación de una emisión protegida para su ulterior reproducción o distribución.

Art. 249. Delitos contra señales satelitales protegidas
Quien contraviniendo la ley de la materia y con el propósito de obtener un beneficio económico para sí o para un tercero, realice cualquiera de los siguientes actos sin autorización escrita del titular del derecho:
La retransmisión o distribución al público de una señal portadora de programas, sea por medios alámbricos o inalámbricos u otro medio o procedimiento similar.
La decodificación de una señal codificada portadora de programas;
La fijación o reproducción de las emisiones;
La fabricación, ensamblaje, modificación, importación, exportación, venta, instalación, mantenimiento, arrendamiento o cualquier otra forma de distribución o comercialización de dispositivos o sistemas que sirvan para decodificar una señal codificada portadora de programas.
El que incurra en cualquiera de las conductas anteriormente señaladas, será sancionado con prisión de uno a tres años o de trescientos a quinientos días multa e inhabilitación especial por el mismo período para ejercer el cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva.

Art. 250. Protección de programas de computación
Será sancionado de trescientos a quinientos días multa o prisión de uno a tres años e inhabilitación especial por el mismo período para ejercer cargo, profesión, oficio, industria o comercio relacionado con la conducta delictiva, quien contraviniendo la ley de la materia fabrique, distribuya o venda mecanismos o sistemas que permitan o faciliten la supresión no autorizada de dispositivos técnicos que se hayan utilizado para evitar la reproducción de programas de computación.
Asamblea Nacional. Proyecto de Ley No. 641, Código Penal, aprobado el 13 de noviembre

Estaba oculto en casa de Los Altos de Ticomo

Cae «madre» de los telepuertos

** Funcionaria del PMA, de origen haitiano, introdujo los equipos y es la madre del haitiano que aparecía como gerente de la fachada NICASAL*

** ENITEL presentó ayer acusación formal en un Juzgado de Distrito capitalino contra siete de los hasta ahora implicados*

** También quebrados otros dos «satélites» del telepuerto 'madre', ubicados en residencias de aparente normalidad*

Especialistas de ENITEL y la Policía Económica inspeccionan los equipos encontrados en una casa de Los Altos de Ticomo, donde según expertos, estaba la «mamacita» de los telepuertos, con tecnología autónoma capaz de recibir, distribuir y enviar por sí sola las llamadas pirateadas al sistema nacional de telecomunicaciones. (Foto: Moisés González Silva)

—KARLA CASTILLO, LIZBETH GARCIA Y OCTAVIO ENRIQUEZ—

Managua

La Policía Económica y el equipo especializado de ENITEL cayeron ayer sobre la «madre» de todos los telepuertos, el que estaba oculto en una casa ubicada en Los Altos de Ticomo y, al parecer, era el centro de la red delincuencial que logró apropiarse de aproximadamente 50 millones de córdobas del pueblo nicaragüense.

El telepuerto «madre» no necesitaba de operarios porque su sofisticado módem satelital es capaz de recibir, distribuir y enviar las llamadas, a través de 20 líneas telefónicas, hacia o desde sus filiales, dos de las cuales también fueron descubiertas la tarde de ayer, en lujosas pero vacías casas de Batahola y Bolonia.

Por parte de la Empresa Nicaragüense de Telecomunicaciones coordinaba el operativo contra los telepuertos el señor Michael Damha Wheelock, director del Centro de Coordinación Operativa de Emergencia, CECOE, ente especializado que recientemente fue apertrechado con equipos carísimos para detectar anomalías delincuenciales en la red de telecomunicaciones nacionales.

LOS CORSARIOS Y EL PMA

Aparentemente «los tentáculos» de los «corsarios de las telecomunicaciones» llegaron hasta el Programa Mundial de Alimentos (PMA) de las Naciones Unidas en Nicaragua porque una funcionaria del mismo introdujo al país los equipos encontrados en el telepuerto madre que la Policía «quebró» ayer.

La funcionaria, de nacionalidad haitiana del PMA, fue identificada como Magaly Hernández, quien no fue acusada por los delitos de defraudación, estafa, fraude y asociación e instigación para delinquir, pero sí fue mencionada en la formal acusación que contra siete personas presentó ayer tarde la compañía telefónica ante el Juez Séptimo de Distrito del Crimen de Managua, por medio de su apoderado legal, Rafael Godínez.

Magaly Hernández, según la acusación de ENITEL, es la madre de Pierre Stephane Sajaous, el haitiano gerente general de la empresa Nicasal, la que supuestamente servía de fachada a uno de los tres telepuertos ilegales que la Policía desmanteló el pasado lunes.

La acusación revela que el trece de julio de 1999 Magaly Hernández introdujo al país, mediante pólizas aduaneras número 2443862 y 107794-01, equipos sofisticados de comunicación satelital incautado por las autoridades este martes en el telepuerto madre, que supuestamente era el corazón del accionar del resto de telepuertos.

Las autoridades encontraron en el «telepuerto madre» 20 antenas de comunicación satelital marca Senao; computadoras que estaban conectadas con la estación terrena y que eran utilizadas para bajar la señal de satélite y otros equipos que llegaron al país gracias a doña Magaly Hernández.

No obstante, la acusación de ENITEL no específica si ella usó su cargo dentro del PMA para facilitar su introducción al país del equipo que aparentemente eran para las operaciones de la empresa de su hijo Pierre Stepane Sajous. Seguramente el juez de la causa o las mismas autoridades de ENITEL solicitarán que sea llamada a declarar en el juicio.

EN ESTADOS UNIDOS SE OFERTAN LIBREMENTE

Damha Wheelock señaló que los propietarios de los telepuertos se aprovechan de las libertades que Estados Unidos permite en las comunicaciones, para promover allá un servicio de llamadas a nuestro país más barato que el de ENITEL. «Así, cualquiera aprovecha la rebaja y hace uso del telepuerto», recalca el director del CECOE.

En la casa de Los Altos de Ticomo fue descubierta una pana parabólica centralizada, dentro de la piscina, pero cubierta por un techo de zinc, madera y plástico, evidentemente construido por los propietarios del telepuerto, para ocultar su delito, a espaldas del dueño de la vivienda, quien nada tiene que ver con el asunto.

El funcionario de ENITEL valoró que el equipo recientemente adquirido para detectar los telepuertos, ha apoyado la ardua labor del CECOE, lo que se evidencia con la eficacia con que se han descubierto media docena de estos negocios ilícitos.

Los otros dos telepuertos descubiertos y «quebrados» por la tarde estaban situados en residencias con apariencia normal, que no despertaban sospecha alguna. Uno, del Ministerio de Defensa 20 varas Arriba, en Bolonia, y el otro, de la

Embajada USA una cuadra Abajo y cuatro cuadras al Lago, en Batahola Norte, donde se descubrió dos líneas con dos monocanales, una antena Yaggi y una onda, instrumentos propios del «pirateo» de llamadas internacionales. Ninguna de estas casas tenía siquiera una silla para que el vigilante se sentara.

Estos aparentemente tienen relación con los tres telepuertos descubiertos el lunes, por lo que suman más de doce líneas telefónicas las que ENITEL sacó de operación.

Según Damha Wheelock, estos telepuertos fueron detectados y «quebrados» porque recibieron llamadas de Estados Unidos. En el telepuerto de Batahola Norte, la Policía entrevistó al señor Victoriano Sánchez, quien estaba empleado como vigilante, el que afirma que fue contratado por un hombre de acento extranjero, moreno, alto, joven, que le pagaba 600 córdobas al mes por su servicio.

La casa de Los Altos de Ticomo donde estaba el cerebro de los seis telepuertos «quebrados» en las últimas horas. (Foto: Moisés González Silva).

Esa descripción coincide con la que dio el señor Carlos Hernández, quien señala que devengaba un sueldo de 1,600 córdobas al mes, por permanecer día y noche en la casa de Altos de Ticomo, donde su patrón -aparentemente el mismo joven extranjero, alto, etc.- le decía que tenía un servicio de llamadas a los departamentos.

El hombre descrito por ambos vigilantes al parecer es el haitiano Pierre Eduard Stefan, quien fue detenido el lunes, al ser «quebrado» el telepuerto que se parapetaba tras una fachada de agencia de envíos de remesas -NICASAL-, de su propiedad.

Las pérdidas preliminares por el accionar de los corsarios de las comunicaciones fueron tasadas en 5 millones 450 mil córdobas con 493 centavos.

Esa cifra corresponde a la facturación de 435 mil 813.20 minutos de llamadas internacionales no facturadas en cinco de los diez números telefónicos con que operaban los telepuertos, revela el informe que Nils Jensen, gerente de informática, remitió a la gerencia de ENITEL.

No obstante, técnicos de ENITEL reiteraron que las cifras de pérdidas totales por el tráfico ilegal de llamadas internacionales podría andar por los 50 millones de córdobas, porque los telepuertos trabajaban las 24 horas del día sin interrupciones y realizaban un promedio de 100 llamadas por hora.

Entre los señalados por ENITEL por su supuesto involucramiento en las operaciones ilegales de los telepuertos se encuentran Ricardo Eduard, Iván Zenny, Pierre Sajous, Enrique Delgado Alvarado Tapia, Jeanne Delgado de Ulvert, Iván Kauffman Miranda, Bismarck Mena Tapia y tres personas más y para todos ellos solicitaron al juez retención migratoria, circulado y orden de captura con allanamiento.

Hasta ayer la Policía aún no había capturado al total de involucrados en el caso ni había remitido al único detenido, Pierre Eduard Stefan, quien aparentemente también es familiar de la funcionaria menor y administrativa del PMA, quien tiene dos años de estar en Nicaragua y 20 años de carrera en el servicio internacional para el organismo de Naciones Unidas.

PMA TOMA DISTANCIA

La vocera del PMA, Olga Moraga, señaló que desconocían por qué y para qué Magaly Hernández introdujo al país los equipos, pero sí señaló que no eran para el PMA.

Moraga lamentó la situación que está viviendo Hernández y señaló que si la autoridad determina que ella es responsable de algún hecho o ha actuado de manera irregular, tendrán que demostrarlo.

La vocera indicó que la funcionaria del PMA no tiene inmunidad diplomática, pero sí goza de algunos privilegios en virtud de acuerdos internacionales que cubren a los que trabajan en el servicio exterior para Naciones Unidas. Vale decir que Magaly Hernández se encarga de velar por aspectos financieros relacionados a los proyectos humanitarios.

Se sospecha que sacó equipos antes que llegara la Policía

Capturan a implicado en telepuerto

–ROBERTO COLLADO NARVAEZ –
Managua

Ayer en horas del mediodía, la Dirección de Investigaciones Económicas de la Policía Nacional capturó a uno de los presuntos involucrados en el Telepuerto que operaba desde una casa del barrio Ocho de Marzo, en las cercanías al mercado Iván Montenegro.

Una radioemisora informó ayer de última hora que el nombre del detenido corresponde al de Norman Arturo Bonilla, de 34 años, habitante del anexo a la colonia Miguel Gutiérrez y de quien se presume sea el mismo que sacó los equipos utilizados en el Telepuerto antes que los ingenieros de ENITEL llegaran a la casa donde funcionaban las líneas piratas.

El sitio donde funcionaba el Telepuerto fue localizado en las cercanías donde antes funcionaba una sucursal de ENITEL. Los ingenieros a cargo de la investigación fueron alarmados por miles de llamadas que venían rastreando en la zona cercana a los semáforos del mercado Iván Montenegro y cuyos registros no aparecían en el inventario de servicios telefónicos de la empresa.

COMISIONADO CONFIRMA DETENCIÓN

La detención de Bonilla fue confirmada por el comisionado Carlos Bendaña quien apuntó que el operativo es producto de una investigación exhaustiva por parte de los miembros de la Policía Nacional.

Además, anotó el oficial, hay testigos que aseguran que este señor fue visto en la casa donde funcionó el Telepuerto en más de una ocasión y no se descarta que el mismo haya sido el que «voló» con los aparatos con que pirateaban las llamadas.

Por otro lado, las investigaciones policiales llevaron a descubrir que Bonilla mantenía vínculos de trabajo con Carlos Pérez Hernández, presunto cabecilla de uno de los tantos Telepuertos que han funcionado en Nicaragua.

Bonilla, al momento de su detención, negó algún vínculo con Pérez Hernández, pero según las pesquisas policiales, el mismo Hernández le había cedido una casa frente al colegio La Salle. Asimismo, las investigaciones comprobaron que Bonilla le hacía trabajos de consultoría a Hernández.

«Lo más seguro es que en este nuevo caso haya sido el mismo Bonilla el que consiguió los equipos con que operaba el Telepuerto del barrio Ocho de Marzo. Pero eso lo sabremos con más seguridad con las próximas indagaciones», dijo el comisionado Carlos Bendaña.

DETENIDO NO DICE NADA

Desde la llegada de la Policía ayer en horas del mediodía, Bonilla negó saber algo sobre las razonas de su detención y aseguró que él nada tiene que ver con «el famoso Telepuerto», desde donde se operaban las más de 20 líneas piratas del barrio Ocho de Marzo.

Según la fuente policial, el detenido deberá rendir su declaración en el Juzgado Primero del crimen hoy en horas de la mañana, donde será interrogado para definir su participación o no en el Telepuerto desarticulado la semana pasada.

La perniciosa actividad de los telepuertos

El funcionamiento de ocho telepuertos ilegales ha causado a Nicaragua pérdidas superiores a los 54 millones de córdobas

Jorge Loásiga
jorge.loasiga@laprensa.com.ni

La mayoría de las ocho causas judiciales abiertas en contra de los acusados por operar ilegalmente los ocho telepuertos que han sido descubiertos desde 1997 por la Empresa Nicaragüense de Telecomunicaciones, han sido cerradas por falta de tipificación de delitos. Una propuesta de reforma a la Ley de Telecomunicaciones sugiere la imposición de multas y penas carcelarias en contra de los que operen telepuertos piratas.

JINOTEPE

La historia de los telepuertos ilegales en Nicaragua inicia en julio de 1997, cuando la Policía Nacional y autoridades de la Empresa Nicaragüense de Telecomunicaciones (Enitel) descubren, en Jinotepe, la primera de esas empresas que operaba llamadas

internacionales de forma ilegal y por el método conocido como By-Pass.

En ese mismo año también iniciaron operaciones cuatro telepuertos legalmente autorizados por Telcor y Enitel.

En los archivos de la Policía se menciona que en el caso de Jinotepe se procesó a una mujer llamada Ana Matilde Avilés Morales, quien al final del juicio fue sobreseída definitivamente, es decir, fue absuelta de culpa por los delitos de estafa y defraudación en contra de Enitel de los que se la acusaba.

COINSA

Posteriormente, en agosto de 1998 se detecta en la Colonia Centroamérica, en la casa número A-45 un telepuerto legalizado, pero que según Enitel realizaba operaciones de transmisión de voz de forma ilegal.

Esta empresa se denominaba Comunicaciones Inalámbricas S.A., Coinsa, cuyo accionista mayoritario era Víctor Martínez Quintana.

La empresa fue legalmente constituida en 1997 con un capital de 10,000 córdobas. Martínez invirtió sólo en los equipos de la estación terrena 500,000 dólares más los gastos de introducción y pagos aduaneros que ascendían a casi 100,000 dólares.

Enitel calculó en esos días pérdidas económicas estimadas en 380,000 dólares mensuales. Coinsa operó durante tres meses.

Martínez finalmente fue sobreseído definitivamente por la Juez Segundo de Distrito del Crimen de Managua, Orietta Banevides. La jueza no encontró ningún tipo de delito para procesar a Martínez, quien firmó una escritura de dación de pago en la que se comprometió a entregar en pago a Enitel los equipos que fueron incautados, valorados en 500,000 dólares.

Telscape, la empresa que le brindaba el servicio de satélite a Coinsa, inició en febrero de 1999 un juicio contra Martínez por el delito de estelionato, por haber entregado en pago algo que según Telscape no le pertenecía, en vista de que los equipos le habían sido entregados en consignación para que fueran operados.

Telscape es una empresa de Texas, Houston, Estados Unidos, que brinda servicios de telecomunicaciones vía satélite a empresas en Latinoamérica.

Es decir, a través de esta empresa norteamericana es que supuestamente Coinsa "bypaseaba'' las llamadas.

Hubo una reunión entre los abogados de Telscape, Enitel y Martínez. La misma se realizó frente a la Casa del Café en Managua, donde está ubicada la Oficina de Leyes F.A.A. Arias & Muñoz, representada por Alvaro Peralta y Pedro Muñoz.

Quien representaba a Martínez era el abogado Ramón Rojas.

En la mencionada reunión se acordó que Telscape pagaría a Enitel el supuesto daño ocasionado a la telefónica nicaragüense por Coinsa para que ésta devolviera los equipos.

Sin embargo, Telscape abrió el juicio contra Martínez y lo abandonó en julio de 1999. Teóricamente Telscape no ha abandonado la causa y ésta se mantiene abierta.

Martínez, por su parte, asegura que todo lo que hizo Enitel fue ilegal, pues él tenía todos los permisos y según él hay intereses oscuros que no permiten el desarrollo de las empresas de comunicaciones en Nicaragua.

CCM

En enero de 1999 es descubierta la empresa Tec Data Comunicaciones S.A. que operaba en el módulo B-19 del Centro Comercial Managua y que causó pérdidas económicas a Enitel por el orden de los 144,108,016 dólares.

Para realizar sus operaciones rentaron a Telematix de Enitel un par de canales para procesar datos vía satélite y con un multiplicador de canales recibían voz que la hacían llegar desde Estados Unidos por 15 líneas telefónicas. En este caso no hubo detenidos y por tanto no hubo proceso judicial.

KALIM HABED

El 15 de junio de 1999 la Policía Nacional detectó un telepuerto ubicado en el edificio Penta de Managua. En esa ocasión Enitel fue víctima de una estafa que ascendía a 15 millones de córdobas. Los piratas de la telefonía enlazaban llamadas de distintas partes del mundo.

El jefe de esta operación era el beliceño/árabe, Kalim Habed. Éste contrató a las salvadoreñas Verónica Isabel Alvarez, Maritza Castellón López y Gretel María Mendieta y a los nicaragüenses Nery Alemán Méndez y Alonso Laguna. Aunque el Juez Séptimo de Distrito del Crimen de Managua, Sabino Hernández, dictó auto de prisión contra los implicados, un jurado de conciencia los encontró inocentes.

COMCASA/JAMAR

El ocho de julio de 1999 la Policía Nacional detectó en las inmediaciones de las empresas de beeper Comunicaciones Centroamericanas S.A. (Comcasa) y la Ferretería Jamar S.A., ubicadas en el kilómetro tres de la carretera norte, un nuevo telepuerto. En este caso se investigó a Gonzalo Meneses Burgos, asesor del entonces Presidente Ejecutivo de Enitel, Jorge Solís y Regis Delgadillo Porras, gerente de Comcasa, así como a Belford Jarquín, propietario de la Ferretería Jamar S.A. El caso fue remitido al Juzgado Séptimo de Distrito del Crimen de Managua, pero no prosperó y los mismos fueron sobreseídos.

PLAZA INTER

En noviembre de 1999 las autoridades policiales descubrieron un telepuerto que operaba en el módulo 2-H de la Plaza Inter, bajo el nombre de Internet Security Sistema Sociedad Anónima (ISS,SA).

El telepuerto, según denuncia de Enitel, desde septiembre de ese año hasta su descubrimiento, causó perjuicios económicos a la telefónica hasta por 2,000,000 de córdobas ''pirateando'' llamadas telefónicas.

El jefe de la operación era el guatemalteco Juan Pablo Galindo Jerez, quien trabajaba con Edgar Monterroso Godoy. Los guatemaltecos fueron condenados a seis y 12 años de prisión respectivamente por los delitos de estafa, defraudación, y asociación ilícita para delinquir. Sólo Monterroso cumple la condena. Galindo se encuentra prófugo de la justicia nicaragüense.

OCHO DE MARZO

En febrero del año 2000 la Policía Nacional descubrió otro telepuerto que sangró a Enitel con 35,000,000 de córdobas a través de 21 líneas telefónicas que estaban instaladas en las cercanías del Mercado 'Iván Montenegro', conectadas a una antigua sucursal de ENITEL, según la denuncia de la institución.

En este caso se procesó a Silvia Elena Ortiz Jirón y Rubén Arturo Bonilla Eslatiff, Guillermo Requene, Eduardo Fletes Solís, Guadalupe Miranda, Rubén Jesús Sequeira Cabrera y Karla Christina Meneses.

Para operar crearon cinco empresas fantasmas en las que Ortiz tenía participación accionaria. Estas empresas eran: Ortiz Fletes y Compañía Limitada, conocida como Networt Mundiales (Netmun); Fletes Miranda Comercial y Compañía Limitada (Agrosin); Sequeira Miranda Comercial y Compañía Limitada (Terras Constructores); Comercio Centroamérica (Concan); Contratistas Industriales y Comerciales; Exportadores Técnica e Industrial (Extin); Florida Real Estate (Floreal); Importadora de Equipos Industriales; Inversiones Centella y Redes Mundiales (Remun).

Las líneas telefónicas fueron reconcentradas en un solo cable y conectadas a una antena parabólica en el Barrio 8 de Marzo; para ello también utilizaron bancos de líneas telefónicas ubicados en la antigua sucursal de Enitel en el Mercado 'Iván Montenegro'. La casa donde operaba el telepuerto pertenecía a Guillermo Requene.

COLONIA "CHRISTIAN PEREZ"

El último telepuerto desmantelado por las autoridades policiales fue descubierto contiguo a la Pizza Valentis, de la Colonia 'Christian Pérez', el que causó pérdidas de hasta dos millones de córdobas a Enitel, con 20 líneas telefónicas que supuestamente fueron autorizadas por funcionarios de Enitel.

En este caso se detuvo a José Antonio Zamora Cruz, Carlos Dionisio Suazo, Wilfredo Ramón Parrales Quintero y Lucía del Socorro Ramírez López.

Cae telepuerto en Rivas

* Era una sociedad de dos rivenses y un tico que se dieron a la fuga
* Policía dice que era más sofisticado que los que se han quebrado en Managua

Lesber Quintero | lquintero@elnuevodiario.com.ni

Éste era el equipo que usaban dos rivenses y un tico para hacer funcionar un telepuerto pirata.

RIVAS

Un telepuerto pirata que operaba a escasas dos cuadras en dirección oeste de la delegación departamental de la Policía de Rivas, fue desmantelado este 23 de enero durante un operativo sorpresa de las autoridades, que siguen la pista de dos rivenses y un costarricense responsables del ilícito negocio, que se estima dejó pérdidas de 192 mil dólares en un mes.

De acuerdo con un informe de Auxilio Judicial de la Policía rivense, los responsables del telepuerto pirata son los hermanos Camilo Gaspar y Denis Alberto Lara Guadamuz, y el tico Jairo Gutiérrez Toruño. Los tres formaron la sociedad "Lara Gutiérrez Compañía Limitada", que empezó a operar ilegalmente desde octubre de 2007, teniendo como oficina un pequeño cuarto.

Según declaraciones del jefe de Auxilio Judicial, subcomisionado César Useda, estos tres sujetos adquirieron con la empresa Enitel un contrato para crear un "centro de llamadas" destinadas a clientes que urgían pedir vía telefónica trasferencias de mercadería.

No obstante, lo que realmente hacían los hermanos y el tico era convertir en llamadas locales las realizadas de Estados Unidos a Nicaragua, cometiendo de esta manera los delitos de estafa, evasión fiscal y asociación ilícita para delinquir, según el informe de la Policía.

Para dicha actividad, los tres socios del telepuerto usaban 48 números convencionales, entre ellos el 563-4636 y el 563-0862. Entre todos estos números se contabilizó en apenas doce días un total de 365 mil 611 minutos en llamadas recibidas desde Estado Unidos, cuyo valor es 0.12 centavos dólar el minuto, por lo que la pérdida en ese corto período es de 43 mil dólares, ya que gracias al truco del tico y de los dos hermanos, las llamadas las hacían pasar como locales.

Sin embargo, se estima que la pérdida será mayor al analizar las llamadas que se recibieron en todo un mes, ya que en todo ese período se cree que las pérdidas rondan los 192 mil dólares.

De acuerdo con el subcomisionado Useda, durante el allanamiento realizado al

telepuerto, ubicado de la Farmacia Miranda 50 metros al oeste, sólo se encontró a Massiel Gómez Fariñas, de 26 años, y cónyuge de Camilo. La misma no fue detenida, pero sí se ocupó un equipo Reuter, dos multiplesores moduladores, un modem, una batería, un teléfono, 48 cajas de terminales telefónicas, 6 mil 380 dólares y un cable telefónico de cien pares, así como documentación.

En el informe policial se señala que es a partir del 20 de diciembre que le vienen dando seguimiento al telepuerto pirata, catalogado por el subcomisionado Useda como uno de los más sofisticados de los que se han quebrado en toda Nicaragua.

Las sospechas del telepuerto se dieron porque el 20 de diciembre la empresa Enitel detectó anomalías, relacionadas con prácticas de defraudación que afectaban los ingresos provenientes de las llamadas internacionales originadas desde Estados Unidos, y que evadían los pagos correspondientes de los teléfonos convencionales, desde cuyas líneas se gestaba el ilícito.

Según Useda, los propietarios de las líneas convencionales que eran usadas para cometer dicha actividad no tienen nada que ver con el fraude, ya que ellos pagaban sus llamadas normalmente, pero el dinero por dicha comunicación quedaba en los bolsillos de los dos hermanos y del tico, y no en Enitel.

Operaba con 100 líneas de Enitel y 100 de Movistar

Cae telepuerto que estafaba a gigantes de comunicaciones

* Auxilio Judicial lo desmanteló ayer, era propiedad de un norteamericano y estaba ubicado en Plaza King's Palace, en Carretera a Masaya
* Pérdidas de empresas se consideran millonarias, sin embargo, el ente "regulador" no sabe nada del asunto

Nery García | ngarcia@elnuevodiario.com.ni

ÓSCAR CANTARERO / END Parte de los equipos que la Policía Nacional incautó a la empresa Amwy Doing S.A.

Efectivos de la Dirección de Auxilio Judicial, de la Policía Nacional, desmantelaron este viernes un telepuerto ilegal, propiedad del norteamericano John Russell Martins, quien presuntamente utilizaba unas 200 líneas de teléfonos celulares para realizar llamadas al exterior, burlando los controles de la Empresa Nicaragüense de Telecomunicaciones (Enitel) y Telefónica Movistar, y sin tener autorización del Instituto Nicaragüense de Telecomunicaciones y Correos (Telcor).

Rafael Godínez Flores, subgerente antifraude de Enitel, explicó que el operativo lo realizaron los efectivos policiales, luego de que la juez Cuarto del Distrito Penal de Audiencia de Managua, Martha Lorena Martínez, ordenara un allanamiento en el módulo diez de la Plaza King´s Palace, en el kilómetro cinco y medio de la Carretera a Masaya, en donde operaba una empresa denominada Amwy Doing S.A., cuyo presidente es Russell Martins.

"Estaban realizando llamadas telefónicas internacionales de carácter fraudulento e ilegal. Ellos (Amwy Doing S.A.) estaban utilizando sus propios sistemas que evaden los controles que Enitel tiene sobre las comunicaciones nacionales e internacionales, y cursan ese tráfico de llamada sin pagárselo a la empresa", declaró Godínez Flores, quien recordó que esa anomalía es sancionada por el Código Penal, que la tipifica como aprovechamiento indebido del fluido de telecomunicaciones.

Agregó que desde el 24 de marzo pasado, Amwy Doing operaba el telepuerto, a pesar de que según la constitución de esta compañía precisa que se dedica al comercio de "productos varios", según dijo Godínez Flores, quien relató que Russell Martins confesó que los aparatos fueron transportados desde Costa Rica hacia Nicaragua, pero desconoce a cuánto asciende su valor.

Pérdidas millonarias

El personero de Enitel comentó que se trata del primer caso en este año, sin embargo, recordó que en diciembre pasado también la Dirección Judicial de Auxilio Judicial desmanteló otros telepuertos piratas, uno de ellos operaba en el Edificio "Armando Guido".

"Ha habido casos relevantes, como uno en el que perdimos 50 millones de córdobas, y en los últimos dos casos que sucedieron en diciembre, fueron de 50 mil dólares, y en el otro 35 mil dólares, pero en este (Amwy Doing S.A.) todavía no sabemos", indicó Godínez Flores.

En el allanamiento se encontraba Russell Martins, pero evitó dar declaraciones a este rotativo.

Un ente regulador que no regula

EL NUEVO DIARIO conoció que, en total, Amwy Doing intervenía 200 líneas de teléfonos celulares, de las cuales 100 son de Enitel y 100 de Movistar, por lo que intentamos comunicarnos con los ejecutivos de la última empresa, pero nos indicaron que será hasta el lunes que darán "una posición oficial".

Asimismo, nos comunicamos con Lucía Castillo, del área de Relaciones Públicas de Telcor, y admitió que el ente regulador no tenía información de ningún caso de telepuerto que operara de manera ilegal, y menos de que la Dirección de Auxilio Judicial de la Policía hiciera algún tipo de allanamiento este viernes. Sin embargo, dijo que en caso supieran sobre ese tema nos regresaría la llamada, lo que no sucedió.

Por su parte, Godínez Flores manifestó que la Policía trasladaría a Russell Martins a la Dirección de Auxilio Judicial para ponerlo a la orden del Ministerio Público, mientras hacen una auditoría para conocer a cuánto ascienden las pérdidas que Amwy Doing provocó a Enitel.

Una Directiva de la UE acaba con las lagunas

Los programas informáticos entran en la élite de la protección de los derechos de autor **Javier Ardalán.**

Los derechos de autor de los programas de ordenador han pasado a convertirse en objeto de especial protección para la Unión Europea, tras la entrada en vigor de la Directiva 2009/24/CE, de 23 de abril, que ha entrado en vigor el pasado miércoles, 6 de mayo. Según establece la nueva normativa, las copias ilegítimas de programas de ordenador podrán ser confiscadas con arreglo a la legislación del Estado miembro correspondiente así como los medios para violar las protecciones para evitar las copias ilegales y los medios técnicos utilizados para ello. En España existe un vacío enorme en la regulación en todos los temas relacionados con las nuevas tecnologías y, muy especialmente, en lo que afecta a la defensa de la propiedad intelectual.

En un reciente debate organizado por BSA (Business Software Alliance), entidad que agrupa a los fabricantes de software, magistrado del Tribunal Supremo José Manuel Maza, denunciaba que el tipo está muy difusamente descrito en el Código Penal y tampoco aportan mucho otras regulaciones colindantes como la Ley de Conservación de Datos que, en opinión de los ponentes, impide la investigación de delitos contra la propiedad intelectual en la Red, por la protección del derecho fundamental a la intimidad de los usuarios.

Uno de los principales objetivos de esta directiva es anular cualquier legislación estatal de los países comunitarios que pueda plantear que permita la descompilación o impida las excepciones establecidas en la presente Directiva

sobre la realización de una copia de salvaguardia o para observar, estudiar o verificar el funcionamiento de un programa.

A este respecto, cabe señalar que Javier Ribas, socio de Landwell-PwC, uno de los primeros temas que habría que plantearse es eliminar la Circular 1/2006 de la Fiscalía General del Estado que ha promovido la idea de que el intercambio de archivos protegidos por derechos de autor no es un delito.

Hasta ahora existían en la Unión Europea multitud de diferencias, sobre la protección jurídica de los programas de ordenador estatales, lo que tanto para la Comisión Europea como para el Parlamento de Estrasburgo han venido efectos negativos y directos sobre el funcionamiento del mercado interior en lo relativo a los programas de ordenador.

A los efectos de la presente Directiva, el término «programa de ordenador» incluye programas en cualquier forma, incluso los que están incorporados en el hardware.

Este término designa también el trabajo preparatorio de concepción que conduce al desarrollo de un programa de ordenador, siempre que la naturaleza del trabajo preparatorio sea tal que más tarde pueda originar un programa de ordenador.

El término «programa de ordenador» en la nueva directiva incluye programas en cualquier forma, incluso los que están incorporados en el hardware y el trabajo preparatorio de concepción que conduce al desarrollo de un programa de ordenador, siempre que la naturaleza del trabajo preparatorio sea tal que más tarde pueda originar un programa de ordenador.

La normativa impide que la información obtenida de un programa informático se utilice para fines distintos del logro de la interoperabilidad del programa de ordenador creado de forma independiente; que se comunique a terceros, salvo cuando sea necesario a efectos de interoperabilidad del programa de ordenador; o se utilice para el desarrollo, producción o comercialización de un programa de ordenador que resulte ser una copia del programa original o para cualquier otro acto que infrinja los derechos de autor.

Las legislaciones nacionales deben adoptar medidas adecuadas contra las personas que pongan en circulación una copia de un programa de ordenador conociendo o pudiendo suponer su naturaleza ilegítima; la tenencia con fines comerciales de una copia de un programa de ordenador, conociendo o pudiendo suponer su naturaleza ilegítima, o la puesta en circulación o tenencia con fines comerciales de cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador.

Dos imputados por estafar más de 3.000 euros por Internet

Noticias Relacionadas

- La Policía Nacional de Albacete detiene a los dos presuntos autores de varias estafas cometidas en Internet (18/02/2009)
- Detenido en Benicarló (Castellón) un individuo acusado de pertenecer a una organización dedicada a estafar por Internet (30/04/2009)
- Sucesos.- Detenido un individuo acusado de pertenecer a una organización dedicada a estafar por Internet (30/04/2009)
- Detenida una pareja acusada de estafar 78.000 euros a clientes de un banco de Barcelona por el método del "phising" (07/05/2009)
- Detenida una pareja acusada de estafar 78.000 a clientes de un banco de Barcelona por el método del "phising" (07/05/2009)

Selección realizada automáticamente por Colbenson

SANTANDER, 7 May. (EUROPA PRESS) -

Agentes de la Guardia Civil de Cantabria han imputado a dos personas, una de Madrid y la otra de Granada, como supuestos autores de un delito de estafa por Internet (phising) por importe de 3.000 euros. Además, se supone su integración en una red organizada.

Según explicaron hoy fuentes de la Benemérita, los agentes --pertenecientes al Equipo de Delitos Informáticos y Tecnológicos (EDITE)-- imputaron el pasado martes a los presuntos estafadores.

En un comunicado, informaron de que la correspondiente denuncia se puso en marzo de 2008 en Suances. A través del representante de una entidad bancaria, la Guardia Civil supo que se habían hecho por Internet dos transferencias bancarias por valor de 1.900 euros y 1.250 euros respectivamente, a terceras personas, sin haberlo realizado el titular de la cuenta bancaria.

Efectivos del EDITE iniciaron la investigación y consideraron que podía tratarse de una presunta estafa por el método 'phising' ya que se supo que alguien se había hecho con las claves del titular de la cuenta bancaria para trabajar por Internet, realizando las dos transferencias.

También se averiguó que los supuestos autores habían realizado las transferencias utilizando una línea de Internet de la ciudad de Algeciras. Con estos y otros datos se dio con los ahora imputados, que actuaban como 'muleros' de una organización presuntamente dedicada a estafas por el método del 'phising'.

Los 'muleros' se encargan de la recepción de las cantidades transferidas fraudulentamente y, tras cobrar una comisión, el resto del dinero lo envían a la organización por medio de sistemas de pagos postales.

REGIÓN

Los delitos informáticos provocan la apertura de una investigación policial a la semana en La Rioja

Los expertos alertan del aumento de las estafas en Internet, con 15 casos en el primer trimestre

ROBERTO GLEZ. LASTRA

Armados y peligrosos. Los delincuentes informáticos se han convertido desde hace unos años en una nueva fuente de preocupación para los investigadores policiales. Ocultos en el anonimato de la Red y con un teclado, un ratón y la banda ancha como afiladas armas, se aprovechan de la ignorancia o inocencia de muchos usuarios para coleccionar víctimas. Sin fronteras y con la ayuda de la heterogénea legislación con la que suelen chocar las Fuerzas de Seguridad, sus negocios florecen en el ciberespacio.

«Las investigaciones son lentas y complicadas», explican expertos consultados por Diario LA RIOJA, que recuerdan que una denuncia en Logroño puede concluir mucho después con una detención en cualquier lugar del mundo. No hay ADN ni restos de sangre, pero el delincuente deja pistas y huellas tan claras como las dactilares.

Durante el año pasado, sólo el Grupo de Delitos Telemáticos de la Guardia Civil en La Rioja realizó una treintena de actuaciones que se saldaron con la detención de 14 personas, 12 de ellas acusadas de pornografía infantil, uno de los delitos que más repugna a la sociedad pero, a la vez, de los más habituales desde el auge de las nuevas tecnologías. Sin embargo, en el primer trimestre de este año se ha detectado un incremento en el número de estafas, subastas y ventas ficticias y las apropiaciones de datos bancarias, phishing y pharming.

Marcados por la crisis

En lo que llevamos del 2009, la Guardia Civil ha desarrollado en La Rioja una media de una actuación semanal debido a los distintos delitos informáticos. Cuatro de las operaciones han sido motivadas por amenazas, injurias y calumnias, el mismo número que en todo el año anterior, que se cerró con dos detenidos. En cuanto a la pornografía infantil, el año ha deparado, hasta la fecha, una única investigación con un detenido, frente a los 12 individuos capturados en las 8 operaciones desarrolladas en todo el 2008 en La Rioja. Sí se detecta un auge, al parecer debido a la crisis económica, en los delitos de estafa y sus variantes. Así, si el año pasado se saldó con 10 actuaciones, el primer trimestre del 2009 acumula ya 9 operativos por estafa, además de cinco denuncias por phishing frente a las nueve del ejercicio anterior.

Mientras, desde la Brigada de Delitos Tecnológicos de la Jefatura Superior de Policía de La Rioja, que no facilita datos estadísticos sobre actuaciones, admiten que con la crisis han aumentado todos los tipos de delitos y señalan las estafas, las ventas falsas, el phishing y las transferencias no autorizadas como las denuncias más habituales. Los investigadores

policiales riojanos, que el año pasado realizaron una veintena de operaciones, explican que su trabajo «se realiza de forma reactiva, una vez que se ha cometido el delito y se ha denunciado, porque rastrear en la Red en busca de anuncios que pudieran ser delictivos nos llevaría siglos».

REGIÓN MURCIA

El inspector jefe de Delitos Tecnológicos dice que el entorno web «carece de fronteras»

08.05.09 -

EP

| MURCIA

El inspector jefe del Grupo de Delitos Tecnológicos, UDEV III, de la Brigada Provincial de Policía Judicial de la Jefatura Superior de Murcia, Carlos Walter Karlsson, señaló ayer que el entorno web «carece de fronteras tecnológicas» durante la clausura de la II Jornada Derecho e Informática bajo el lema *Informática Forense* celebradas en la Universidad Católica San Antonio de Murcia (UCAM).

En este sentido, señaló que «hoy en día no basta con ser buenos policías, y para lograr resultados eficaces en la lucha contra el delito informático es necesario el trabajo coordinado, a nivel nacional e internacional, de los diferentes Cuerpos de Seguridad del Estado, INTERPOL, unidades especiales, brigadas y grupos de investigación tecnológica», según informaron fuentes de la institución docente en un comunicado.

El investigador participó en esta jornada, celebrada en el marco del Master Oficial de Abogacía y Práctica Jurídica, organizada por las titulaciones de Derecho, Informática y Criminología de la Universidad Católica, en colaboración con la Dirección General de la Policía y la Universidad de Oviedo, representada por el experto en Peritaje Informático, Xaviel García Pañiera. Walter Karlsson, analizó durante su intervención los distintos delitos perpetrados al amparo de las nuevas Tecnologías de la Información, como Internet, televisión o la telefonía móvil.