180

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGÓN

"ESTUDIO DOGMÁTICO DEL DELITO DE DAÑO EN PROPIEDAD AJENA POR MEDIO DE LA INTERNET EN PERJUICIO DE TERCERAS PERSONAS, LAS CUALES DEPENDEN DE INSTITUCIONES DEDICADAS A LOS ESTUDIOS E INVESTIGACIÓN EN LAS CIENCIAS MÉDICAS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A:

HÉCTOR JAVIER GUZMÁN HERNÁNDEZ

ASESOR:
LIC. JOSÉ HERNÁNDEZ RODRÍGUEZ

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO, 2002

AGRADECIMIENTOS

A Dios:

Arquitecto universal, ya que sus trazos me permitieron llegar a este día.

A mis padres:

Leticia y Juan José.

Por todo el cariño y empeño que han tenido para hacer de mi y mis hermanos hombres libres y de buenas costumbres.

A mis hermanos:

Juan Antonio, David Víctor Arturo y Jorge Alberto.

Queridos compañeros de toda la vida, No tengo palabras para decirles cuanto los quiero.

A mi Familia:

Por los lazos que me unen a cada uno de ustedes, con la esperanza de que esto nunca cambie.

A Eric:

Con la ilusión de que pronto podamos celebrar lo que hoy esta pasando. Te hecho mucho de menos.

A mis maestros:

Lic. José Hernández Rodríguez y Lic. Raúl Juárez García.

Por el apoyo en la realización del presente trabajo, pero sobre todo por la amistad y fraternidad que me han brindado.

A ti compañera:

Que tal vez no quieras ser reconocida, por el cariño y apoyo en todo momento.

A la "UNAM", "ENEP Aragón":

A todos los maestros por seguir haciendo de la universidad la institución más importante de América Latina, forjadora de profesionistas, hombres y mujeres de bien para la humanidad.

Al colegio Justo Sierra:

Por formarme como alumno, docente y sobre todo por "Educar para la vida"

ÍNDICE

INTRODUCCIÓN. I

CAPÍTULO I. ANTECEDENTES DEL DESARROLLO TECNOLÓGICO.

1.1. Conceptos Generales de la computadora 1

1.2. Antecedentes. 10

1.3. Clasificación de las computadoras 18

1.4. Aplicaciones de la informática 21

CAPÍTULO II. PARTICULARIDADES DE INTERNET.

2.1. Definición de Internet. 25

2.2. Antecedentes Históricos de Internet ..... 26.

2.3. Historia de Internet en México. 31

2.4. Funcionamiento de Internet. 32

CAPÍTULO III. TRANSGRESIONES A TERCEROS POR MEDIO DE LA INFORMÁTICA.

3.1. Concepto de "Delitos Informáticos" 37

3.2. Tipos de Delitos Informáticos. 39

3.3. Hackers y Crackers 43

3.3.1 Víctimas de los Hackers y Crackers. 45

3.3.2 Consecuencias Médicas. 62

3.3.3 Detección de la problemática en el equipo de cómputo 63

3.4. Criptología 68

3.5. Organismos Internacionales que han creado sistemas de prevención..... 72

CAPÍTULO VI. CONTROL EN MÉXICO DE DELITOS INFORMÁTICOS.

4.1. Concepto de daño en propiedad ajena..... 78

4.2. Elementos del delito..... 85

4.3. Sujeto activo y Sujeto pasivo..... 87

4.4. Medios de comisión..... 91

4.5. Legislación Internacional para el control de delitos informáticos. 92

4.6. Legislación en México para el control de delitos informáticos 119

CONCLUSIONES..... 128

BIBLIOGRAFÍA

LEGISLACIONES

INTRODUCCIÓN

El desarrollo que nuestro país ha tenido en los últimos años en materia informática ha sido motivo del surgimiento de muchos y muy diversos tipos de relaciones jurídicas que han requerido, de igual manera, de una cada vez más especializada reglamentación jurídica, tal es el caso del derecho protector de la propiedad intelectual.

Debido a que la ciencia y la tecnología están en constante progreso, se requiere así mismo que la ley se vaya transformando para incluir los aspectos novedosos de la realidad social y el desarrollo tecnológico.

Internet es el nombre de una red mundial de redes de cómputo al servicio de la información e intercomunicación mundial, que se pone al descubierto en México, después de casi 15 años de su aplicación en Estados Unidos.

Indudablemente que su uso en México, inaugura, una nueva era del progreso en nuestro país, en donde apenas el uso de las computadoras no es del todo generalizado, y en donde el derecho a la libertad, información, consignada en nuestra constitución, aún no ha sido objeto de estudios profundos, como los que ahora, con la comercialización de este sistema, tendrán que plantearse los legisladores y el mismo estado mexicano.

El objetivo general de la investigación es analizar y hacer referencia de algunas conductas delictivas que pueden servirse de la tecnología de punta, sobre todo en el campo de la informática: delitos tradicionales que hoy se cometen de forma no tan tradicional, por ello es menester estudiar cómo son cometidos estos delitos y de qué manera podrían ser regulados.

Podemos estudiar un sin número de delitos como son: espionaje, plagio, violación de correspondencia, corrupción de menores, ultrajes a la moral pública, etc. Sin embargo un tema que considero de importancia fundamental es el delito de daño en propiedad ajena; contemplado en él artículo 397 del código penal; el cual considero no regula de manera adecuada el delito antes mencionado, cuando este es cometido por medio de algún virus informático,

que puede dañar desde un archivo hasta el equipo de computo en su totalidad.

Estos virus informáticos como ya todos sabemos se pueden adquirir por diversos medios como son: insertar un disco infectado con un virus o la más frecuente que es por medio de Internet.

Ahora bien ya que sería sumamente complejo estudiar todas y cada una de las posibles victimas de este delito, la investigación fundamentalmente será enfocada a las instituciones dedicadas a los estudios e investigación de las ciencias médicas, caso concreto los laboratorios de estudios clínicos, por ser estas instituciones de importancia radical para la investigación y tratamiento de múltiples enfermedades.

CAPÍTULO I
ANTECEDENTES DEL DESARROLLO TECNOLÓGICO

Ante el inicio del siglo XXI, la intensa competencia mundial y principalmente el surgimiento de nuevas tecnologías de comunicación e información transforman rápidamente a la sociedad, y directa o indirectamente, estos factores tienen un gran impacto en el actuar de las organizaciones y de los gobiernos de los distintos países. Posiblemente somos ahora, testigos del cambio más profundo desde el comienzo de la revolución industrial, y lo que contribuyó al éxito de las empresas en el pasado parece no tener mucho valor en el futuro. Por tal motivo resulta indispensable, para toda organización, la comprensión del "nuevo orden mundial" que deriva de una tercera revolución: "La digital". No basta con sólo mejorar las viejas formas de operación y administración de la era industrial, es importante incorporar elementos de futuro que permitan un desarrollo sustentable de acuerdo a la nueva dinámica social. "Innovar es la clave".

Pero esta innovación ha dado lugar a un nuevo tipo de delitos. Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran relacionadas con la protección a la propiedad intelectual. Por ello, en primer lugar, es conveniente exponer los aspectos relativos a estos temas.

Así. en este capítulo se presentan los aspectos generales sobre la computadora y los antecedentes de la informática.

1.1 CONCEPTOS GENERALES DE LA COMPUTADORA.

Computadora: Máquina compuesta de elementos físicos (en su mayoría de origen electrónico) capaz de aceptar unos datos de entrada, realizar con ellos operaciones lógicas y aritméticas con gran velocidad y precisión, y proporcionar los resultados a través de algún medio de salida; todo ello es llevado a cabo sin la intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en la propia computadora. Por

consiguiente, una computadora puede ser considerada como un sistema que acepta unas entradas (datos e instrucciones) y devuelve unas salidas (datos de salida o resultados). Según esta definición, una calculadora (no programable) no sería una computadora (como algunos afirman), ya que requiere el control directo del usuario y sólo puede realizar operaciones aritméticas. De la propia definición también se deduce que toda computadora siempre actúa con dos tipos de informaciones: datos (que pueden ser de entrada o de salida) e instrucciones.

Dato: Conjunto de símbolos que representan una información de una forma aceptable para ser procesada de alguna forma. Un dato puede ser el peso de una persona (25 Kg.), su R. F. C. (GUHH770831), la superficie de una finca (450 m^2), etc. Los datos, por sí solos, no poseen ninguna utilidad, para ello necesitan de una interpretación (dada por los humanos) que les de sentido.

Programa: Conjunto de órdenes o instrucciones que se le dan a una computadora para realizar un proceso determinado. Las órdenes que integran un programa indican a la computadora las tareas que han de ser realizadas para llevar a cabo el proceso requerido.

ELEMENTOS CONSTITUYENTES DE UN SISTEMA INFORMÁTICO

Hardware: Conjunto de materiales físicos que componen el sistema informático, es decir, la propia computadora, los dispositivos externos a la misma, así como todo material físico relacionado con ellos (conexiones, cables, etc.).

Software: Parte lógica del sistema informático que dota al equipo físico de la capacidad para realizar cualquier tipo de tareas. De acuerdo a esta definición, el software integraría al conjunto de programas ejecutables sobre el hardware junto con los documentos y datos asociados a los mismos.

Personal informático: Conjunto de personas que desempeñan las distintas funciones relacionadas con la utilización y explotación de las computadoras en una determinada empresa u organización.

HARDWARE

La Computadora Central: Es el elemento más importante de la computadora, ya que maneja todo el procesamiento, coordinando y realizando todas las operaciones del sistema informático. Podemos distinguir, a su vez, dos unidades funcionales dentro de la computadora central: la unidad de memoria principal y la unidad central del procesamiento (CPU):

Memoria principal, central o interna: Es el elemento encargado de almacenar los programas y los datos necesarios para que el sistema informático lleve a cabo alguna tarea. Para que un programa pueda ser ejecutado en una computadora, al menos parte del mismo debe encontrarse en memoria principal, junto con los datos que deban ser procesados. Estas memorias presentan gran rapidez y se componen de celdas direccionadas, de forma que cada operación de lectura o escritura en memoria exige la especificación de la dirección sobre la cual se va a realizar dicha operación. Existen dos tipos de memoria principal: la memoria RAM, que permite realizar tanto operaciones de lectura como de escritura y es volátil (si se desconecta el ordenador, se pierde toda la información almacenada), y la memoria ROM, que sólo permite lecturas y es permanente (no necesita ser alimentada con corriente para mantener la información almacenada).

Unidad central de procesamiento (CPU): También denominada procesador, es el elemento encargado del control y ejecución de las operaciones del sistema. Se puede considerar como el cerebro de la computadora y está compuesto, a su vez, de dos unidades:

La unidad de control: Es el elemento encargado de coordinar todas las actividades de la computadora. Para ello, se comunica con todas las demás unidades e interpreta y ejecuta ordenadamente las instrucciones del programa en curso.

La unidad aritmético-lógica (ALU): Está constituida por los circuitos electrónicos necesarios para la realización de operaciones elementales de tipo

aritmético (suma, resta, multiplicación, etc.) y lógico (comparaciones, operación OR, operación AND, etc.).

UNIDADES DE ENTRADA

"Son aquellos dispositivos encargados de aceptar datos de entrada e instrucciones del exterior y transformarlos en señales binarias eléctricas susceptibles de ser procesadas directamente por la computadora".[1] Ejemplos típicos de unidades de entrada son el teclado y el ratón.

Teclado: Los teclados son similares a los de una máquina de escribir, correspondiendo cada tecla a uno o varios caracteres, funciones u órdenes. Para seleccionar uno de los caracteres, puede ser necesario pulsar simultáneamente dos o más teclas, una de ellas correspondiente al carácter (mayúsculas, minúsculas, Alt, etc.). El teclado dispone de un conjunto de teclas agrupadas en 4 bloques.

Teclado principal o alfanumérico: Contiene los caracteres alfabéticos, numéricos y especiales, como en una máquina de escribir convencional, con alguno más.

Teclado numérico: Es habitual que las teclas correspondientes a los dígitos decimales, signos de operaciones básicos y punto decimal estén repetidas para facilitar al usuario la introducción de datos numéricos.

Teclas de gestión de imagen o de control: Sobre la pantalla se visualiza una marca o cursor (indicador de posición). También se suelen denominar con el nombre de teclas del cursor. El cursor indica la posición donde aparecerá el siguiente carácter que tecleemos. Las teclas de gestión de imagen permiten modificar la posición de dicho cursor en la pantalla.

Teclas de función: Normalmente distribuidas en una hilera en la parte

[1] Mora, José Luis. Introducción a la informática. México 1985. Edit Trillas. P.146.

superior del teclado. El número más usual de teclas de función es 12 (Fl, F2,..., F12). Son teclas cuyas funciones están definidas por el usuario o predefinidas por una aplicación. Así, la tecla F1 tiene funciones diferentes dependiendo de la aplicación que se esté ejecutando. En la mayoría de las aplicaciones Windows, por ejemplo, al pulsar la tecla F1 se abre una ventana de ayuda.

Cuando se presiona una tecla, un pequeño chip dentro de la computadora o del teclado, llamado controlador del teclado, se percata de que una tecla ha sido presionada y coloca un código en parte de su memoria, denominada memoria temporal del teclado (buffer), que indica qué tecla fue seleccionada. El controlador envía una petición de interrupción a la CPU y cuando la CPU la acepte pasa el carácter del buffer a la CPU.

El ratón: es un dispositivo de entrada que sirve para introducir información gráfica o seleccionar coordenadas (x,y) de una pantalla. Dispone de uno o más pulsadores con los que el usuario envía ordenes a la computadora, relacionadas con el punto seleccionado en la pantalla. Internamente está constituido por una bola que puede girar libremente y unos rodillos perpendiculares entre sí. Cuando el ratón se desplaza sobre una superficie, la bola se mueve y hace girar los rodillos en un sentido u otro. Esta información es transmitida a través de un cable a la computadora y el programa gestor del ratón puede determinar la distancia, dirección y sentido del desplazamiento desde que se inició el último movimiento. Los ratones detectan movimientos relativos. En la pantalla aparece un cursor que se mueve en el mismo sentido en el que se desplaza el ratón a través de una superficie, indicando el punto sobre el que se actuará.

El dispositivo que acabamos de describir se conoce con el nombre de ratón mecánico, sin embargo existen también los denominados ratones ópticos. A diferencia del ratón mecánico, que puede deslizarse por cualquier superficie que permita el movimiento de su bola, en el ratón óptico el movimiento se tiene que realizar sobre una tablilla especial de material reflectante. El ratón contiene dos focos luminosos que proyectan dos haces sobre la tablilla, la cual los refleja y

pasan a través de dos orificios para ser detectados por un par de fotosensores. Este tipo de ratón es menos propenso a fallos y averías, pero presenta el inconveniente de necesitar la tablilla para el desplazamiento y de ser más caro.

UNIDADES DE SALIDA

Son aquellos dispositivos que devuelven al exterior datos de salida obtenidos como resultado de algún tipo de procesamiento. "Se encargan de transformar las señales binarias procedentes de la computadora central, a cadenas de caracteres o a otro formato comprensible por el humano (gráficos, sonido, etc.). Ejemplos típicos de unidades de salida son los monitores y las impresoras".[2]

Monitor: La forma mas cómoda de recibir información es a través de la vista. Los monitores constituyen el sistema más cómodo y usual de captar las salidas de una computadora.

La imagen de pantalla de la computadora se forma con multitud de puntos denominados puntos de imagen o píxeles. La imagen se forma físicamente con la activación selectiva de unos elementos denominados puntos de pantalla. Un punto de pantalla se iluminará más cuanto mayor sea la activación del elemento correspondiente.

Cuando la pantalla se utiliza para visualizar texto, se considera dividida en celdas con un determinado número de píxeles de ancho y largo para representar un carácter.

Teniendo en cuenta la información a visualizar, hay dos tipos de monitores:

1.-Monitores de caracteres. que actúan en modo texto (sólo pueden visualizar un juego de caracteres preestablecido, como caracteres ASCII).

[2] Ibidem. P. 157.

2.-Monitores gráficos. (el usuario tiene acceso a los pixeles pudiendo representar en ellos dibujos y caracteres),

Impresoras: Son periféricos que escriben la información de salida sobre papel. Junto con el monitor son los dispositivos de salida más utilizados. Existen multitud de tipos y modelos. Se clasifican según dos criterios:

Por el modo de impresión de los caracteres:

Impresoras con impacto. Son aquellas que para imprimir los caracteres precisan golpear sobre el papel el carácter preformado en relieve o configurado en una cabeza de escritura. La ventaja de este tipo de impresoras es que se pueden realizar varias copias simultáneas del documento intercalando papel carbón. Como inconveniente, puede considerarse el excesivo ruido producido con el golpeo.

Impresoras sin impacto. Se eliminan los movimientos mecánicos y el impacto, con lo que se consiguen mayores velocidades y desaparece el ruido. No se pueden obtener copias simultáneas. Utilizan técnicas basadas en fenómenos térmicos, electrostáticos, químicos, así como el rayo láser.

Por el número de caracteres que pueden escribir simultáneamente:

Impresoras de caracteres. Realizan la impresión carácter a carácter de forma secuencial. Son dispositivos lentos que consiguen velocidades de hasta 600 cps.

Impresora de líneas. Realizan la impresión línea a línea, de forma que seleccionando previamente los caracteres que se han de imprimir en una línea, con un único golpe se imprimen simultáneamente todos los caracteres que la componen. Se consideran rápidas, alcanzando velocidades de hasta 2.400 lpm o 5.113 cps.

Impresoras de páginas. Imprimen una página de una vez. Son las más

rápidas. Se consiguen velocidades de 88.000 cps que son aproximadamente 570 ppm (10 pps).

SOFTWARE

El software de un sistema informático está constituido por el conjunto de programas ejecutables en dicho sistema y todo lo relacionado con los mimos. Dentro del software se incluyen: el sistema operativo, las interfaces de usuario, los lenguajes de programación, las herramientas o utilidades, las aplicaciones de cualquier especialidad, tipo o contenido, etc.

Las computadoras tienen la capacidad de realizar muy diversas tareas siempre que tengan el software adecuado. Las computadoras permiten realizar tareas que antes necesitaban un personal muy especializado en diversos campos (mecanografía, delineación, analistas financieros, programadores, etc.) para poder llevarlas a cabo. Actualmente, la gran mayoría de esas tareas pueden ser realizadas mediante una computadora personal, el software adecuado y una persona entrenada mínimamente en ese software.

Una primera clasificación del software nos permite diferenciar dos grandes categorías: software de sistema y Software de aplicación.

SOFTWARE DE SISTEMA

Llamamos software de sistema al conjunto de programas que se encargan de controlar el funcionamiento de los programas que se ejecutan y de la gestión interna de los recursos físicos de la computadora. "Como es natural, el sistema operativo forma parte del software de sistema pero, además, se incluyen aquí el software de programación y el software de diagnóstico y mantenimiento".[3]

Software de programación: Está formado por los programas y utilidades que facilitan la construcción de aplicaciones de usuarios. Aquí incluiríamos a los

[3] Paredes Olea, Héctor. Conceptos básicos de computación. México 1997. Edit. Trillas. P. 30.

intérpretes, los compiladores, los montadores, los módulos de gestión de ficheros, los cargadores, etc.

Software de diagnóstico y mantenimiento: Es el software utilizado por el personal encargado de la puesta a punto de los equipos. Con este software se pretende localizar averías de un periférico o encontrar el mal funcionamiento de un paquete software.

Un ejemplo de prueba de chequeo de la memoria puede consistir en escribir en todas las posiciones de memoria un valor determinado, posteriormente se leen todas estas posiciones y se comprueba donde no coincida el valor leído con el escrito. Esto nos determina las posiciones que se encuentran en un mal estado. Un sistema parecido se puede usar para comprobar la memoria masiva.

SOFTWARE DE APLICACIÓN

"El software de aplicación lo forman los programas que controlan el funcionamiento de la computadora para realizar una tarea específica (esta tarea es denominada normalmente aplicación). Dentro de este tipo de software se incluyen el software estándar y el software a medida".[4]

El software estándar o herramientas informáticas hace referencia a aquellas aplicaciones de uso general especialmente diseñadas para su lanzamiento al mercado. Estas aplicaciones pueden ser utilizadas por gran número de usuarios y sobre diferentes sistemas. Algunas de estas aplicaciones de uso común son el tratamiento de textos, las hojas de cálculo, la gestión de base de datos, comunicaciones, gráficos, los paquetes integrados, etc.

El software a medida está constituido por aquellas aplicaciones específicas que se refieren a actividades más especializadas. En este caso, una aplicación de este tipo es desarrollada para un/unos usuario/s concreto/s y para un sistema

[4] Ibidem. P. 31.

específico. Aquí se incluyen los programas realizados por los propios usuarios, una aplicación de control del tráfico en el área de Londres, un sistema experto para el reconocimiento de yacimientos de minerales, un programa para llevar la contabilidad y la gestión de clientes de una empresa concreta, etc.

1.2. ANTECEDENTES.

El nacimiento de la informática está relacionado con la necesidad que ha sentido el hombre de disponer de un sistema que le permita manejar gran cantidad de información con relativa rapidez así como de efectuar cálculos a gran velocidad y de un modo mecánico que libere de las penosas tareas asociadas con estas actividades. Los primeros antecedentes de sistemas muy rudimentarios, destinados a solventar estos problemas son, por ejemplo:

A) El ábaco.

El ábaco puede ser considerado como la primera herramienta mecánica eficaz para ayudar al cálculo, y aún es muy usado en algunas partes del mundo para muchas tareas sencillas. El ábaco ha sido utilizado (y se utiliza) en tantas culturas diferentes y tan distantes unas de otras que se cree que fue inventado independientemente en cada una de ellas.

En principio, el ábaco no es más que un conjunto de ranuras o varillas en las que se deslizan piezas de piedra o madera que, según la posición y cantidad, permiten realizar fundamentalmente sumas y restas. Sólo en algunas culturas el ábaco se desarrolló lo suficiente para permitir la realización de multiplicaciones, divisiones y potencias.

El conocido ábaco chino (año 1.200 después de J.C., aproximadamente) se compone de un marco atravesado por alambres, en cada uno de ellos, se deslizan siete cuentas, dos arriba de un travesaño central y cinco abajo. Los alambres están en correspondencia con las posiciones de los dígitos en el sistema decimal (unidades, decenas, centenas, etc.) y las cuentas representan dígitos: las

superiores representan cinco y las inferiores uno. Los números se representan entonces con las cuentas más próximas al travesaño central. Por consiguiente, este dispositivo permite realizar cálculos con un número de cifras dependiente del número de varillas que posea.

El ábaco es un calculador nada despreciable. Hoy día es una herramienta que, con un operador bien entrenado, puede sumar columnas de números con mayor rapidez que muchos operadores de calculadoras electrónicas.

El ábaco se constata en Roma, en la India, en la cultura árabe, en la cultura maya, en Rusia, en China (Suan-Pan) y en Japón (Sorobán). Su aparición va generalmente ligada al desarrollo de las matemáticas como metalenguaje.

A comienzos del siglo XVII ya había sido aceptado por muchos países de Europa el sistema decimal, lo que hizo que el uso del abaco se fuese viendo relegado a un segundo plano. "En aquellos tiempos, la multiplicación y la división necesitaban casi un matemático, pero rápidamente estos problemas se iban a solventar gracias a varios matemáticos".[5]

B)Tablas de logaritmos (1615)

Dada la dificultad para realizar operaciones matemáticas como la multiplicación y la división, el matemático John Napier crea las tablas de logaritmos, las cuales permitian realizar multiplicaciones de forma rápida y sencilla. "Diseñó también una calculadora con tarjetas (estructuras de Napier) que permitía multiplicar, y que se puede considerar como un dispositivo intermedio entre el abaco y las primeras calculadoras mecánicas".[6]

C) La máquina de Pascal (1642)

Primer prototipo de calculadora mecánica, que se atribuye al matemático y

[5] Ibidem. P. 188.
[6] Ginnzburg, Mario C. Introducción General a la Informática. Argentina 1999. Edit. UAI. p. 115

filósofo francés Blaise Pascal (1.623-1.662). La máquina aritmética de Pascal (en un principio se denominó pascalina) se basaba en un conjunto de ruedas dentadas y ejes solidarios que simulaba el funcionamiento del abaco. "Algo más tarde, en 1.671, un diseño más elaborado, usando cilindros con dientes de longitud variable, fue desarrollado por el matemático alemán Gottfried Leibniz. (1.646-1.716), convirtiendo la máquina de sumar de Pascal en una máquina capaz de sumar, restar, multiplicar, dividir y obtener raíces".[7]

D) La tarjeta perforada (1804)

La realización automática de un proceso es curiosamente ajena al cálculo automático, y es uno de los procesos de convergencia entre el desarrollo de la máquina y el procesador. Este paso se debe al francés Joseph Marie Jacquard (1.752-1.834), que utilizó un sistema de tarjetas y cintas perforadas. Este sistema sólo fue utilizado en un principio en la industria textil para realizar el control automático de los dibujos y figuras que se habían de tejer en los telares. "Podemos considerar al telar de Jacquard como la primera máquina programada y fue presentada en 1801".[8]

E) La máquina de Babbage (1834)

Charles Babbage, profesor de matemáticas en la Universidad de Cambridge, que concibió una máquina capaz de actuar de diferente manera, según el programa que se le suministrara sobre datos introducidos en forma de fichas perforadas. Dedicó toda su vida y gran parte de su fortuna al desarrollo de esta máquina. "Desgraciadamente, en su época no podía contar con medios eléctricos y mucho menos electrónicos, por lo que sus esfuerzos se encaminaron a la utilización de elementos mecánicos semejantes a las sumadoras calculadoras que, según los modelos de Pascal y Leibniz, se utilizaban en su época".[9]

---

[7] Ibidem.
[8] Ibidem. p. 116.
[9] Ibidem.

Babbage diseñó en 1822 una primera máquina de calcular basada en fundamentos mecánicos para resolver funciones, a la que denominaría máquina de diferencias. Esta máquina no se llegó a fabricar, en parte porque Babbage ya estaba pensando en su segunda máquina.

Poco después, en 1833, Babbage diseñó su segunda máquina, denominada máquina analítica, para producir tablas de navegación. "Esta máquina podía ser programada por medio de tarjetas de cartón perforado (idea que obtuvo de los telares de Jacquard), siendo, además, capaz de almacenar internamente una cantidad de cifras considerable (memoria de 1000 números de 50 cifras con 20 decimales de exactitud). En su diseño se identificaban los cinco elementos básicos propios de la concepción actual del computador: entrada (de tarjetas perforadas), salida (impresión de salida automática), unidad aritmético-lógica (denominada fábrica), unidad de control (disponía de control secuencial del programa) y memoria (denominada almacén).Por consiguiente, esta máquina podía ser considerada como un prototipo de la computadora universal completamente automática, por lo cual en la actualidad se considera a su inventor como el padre de la informática".[10]

F) El código de Hermán Hollerith.

En 1880, el censo estadounidense para esa década fue terminado cuando era tiempo de empezar el de 1890. Esta tardanza se debía a la falta de métodos automáticos que redujesen el trabajo manual. Para paliar este problema, Hermán Hollerith (1860-1929), estadístico norteamericano que trabajaba en la Oficina de Censo de Estados Unidos, concibió un sistema para la codificación y el tratamiento de los datos estadísticos mediante la utilización de tarjetas perforadas. En 1.887, Hollerith produjo un aparato conocido, como la máquina censadora o tabuladora, que permitía reducir el tiempo de tabulación a sólo un octava parte del requerido. La velocidad de clasificación que obtenía era de unas 60 tarjetas por

[10] Ibidem.

minuto. "Esta máquina tuvo gran éxito e hizo posible concluir en menos de tres años el recuento de 1890 (no obstante, esto resulta muy lento para las exigencias de hoy en día). El recuento del año 1.950, hecho con tarjetas perforadas, duró casi dos años".[11]

Después del censo de 1890, hacia 1895, Hollerith adaptó su equipo al uso de los negocios incluyendo en su máquina la operación de sumar, y construyendo un sistema de estadísticas de carga para dos líneas de ferrocarriles. Hollerith fundó en 1896 una compañía para explotar su invento, la Tabuluting Machine Corporation. "Posteriormente, se extendió el uso de las máquinas tabuladoras de Hollerith a otros campos de la industria y el comercio. Se las llamó máquinas de registro unitario (refiriéndose a la tarjeta), ya que todas las máquinas, fuese cual fuese su función, utilizaban el mismo modelo de registro: la tarjeta perforada de Hollerith".[12]

"La empresa del inventor prosperó rápidamente y en 1924, tras varias fusiones, Thomas J. Watson adquiere la empresa de Hollerith y la convierte en la International Bussines Machines, conocida mundialmente como IBM, que durante mucho tiempo, y aún hoy, ha dominado y domina el mercado de los ordenadores electrónicos (computadoras)".[13]

G) La Mark (1937-1944).

En 1937, el profesor de la universidad de Harvard Howard Aiken (1900-1973) comenzó la construcción de una máquina de cálculo automático que combinaba la tecnología del momento con las tarjetas perforadas de Hollerith. El proyecto fue terminado y presentado en Harvard en 1944 con la ayuda de estudiantes graduados de su departamento e ingenieros de IBM. "El resultado obtenido fue el primer calculador digital automático de uso general, que se

[11] Ibidem. p. 117.
[12] Ibidem.
[13] Ibidem.

denominó Calculadora automática controlada secuencialmente (ASCC-Automatic Sequence Controlled Calculator), conocido como la Harvard Mark-I".[14]

"Este mecanismo estaba basado en el uso de relés electromagnéticos, ruedas dentadas y embragues electromecánicos. Por tanto, el Mark-I no era una computadora electrónica, sino que era la primera computadora electromecánica que se construyó y funcionó. En muchos aspectos, era la realización de los sueños de Babbage, ya que disponía de elementos de entrada y de salida (tabuladoras de Hollerith y lectoras de cinta de papel), unidad aritmética, unidad de control y memoria central. No obstante, dicho ordenador no era capaz de multiplicar dos números de veinticinco cifras en menos de cuatro segundos, velocidad bajísima comparada con la de hoy".[15]

H) La ENAC (1946).

En 1946, en la Escuela Moore de Ingeniería Eléctrica de la Universidad de Pennsylvania, y bajo la dirección de un ingeniero eléctrico, J. Presper Eckert, y un físico, John W. Mauchiy, se construyó la primera computadora electrónica de uso general (ABC era de uso específico), el ENIAC (Electronic Numerical Integrator and Compute), para el Ejercito de Estados Unidos. Su destino sería el cálculo rápido de tablas de disparo de artillería. En el equipo de construcción de esta computadora se encontraban J. V. Atanasoff y C. Berry, cuyos estudios y ensayos sobre su calculadora ABC fueron muy importantes para el proyecto ENIAC.

Tanto el Mark-I como el ENIAC determinaban su programa mediante la conexión de multitud de clavijas externas. "Dependiendo de la posición que adoptaran estas clavijas en un tablero, las máquinas efectuaban unos cálculos determinados. Los tubos de vacío también fueron usados en ENIAC. Podía efectuar 300 multiplicaciones por segundo, 300 veces más rápido que cualquier

[14] Ibidem. p. 118.
[15] Ibidem.

dispositivo de su tiempo. No obstante, sus dimensiones eran desorbitadas.

(ocupaba muchísimo espacio, 111 m de volumen y 60 m^2 de superficie, y pesaba 30 toneladas) y su consumo era excesivo (entre 100.000 y 200.000 vatios). Además, el equipo necesitaba ventilación y su mantenimiento era muy costoso".[16]

Los inventores del ENIAC también fundaron una compañía, la Eckert-Mauchly Computer Corporation, que más tarde sería englobada en la Remington Rand, en la que se construiría el primer ordenador comercial: el UNIVAC I. ENIAC fue usada por el ejército hasta 1955, cuando fue colocada en el instituto Smithsoniano.

La ENIAC fue instalada en Aberdeen Proving Ground, y en una visita a este lugar en el verano de 1944, John Van Neumann (1903-1957), consultor del grupo teórico de los Álamos, encargado de resolver los problemas de cálculo relacionados con el proyecto de la primera bomba atómica, tuvo la idea de construir una computadora con programa almacenado, es decir, que la determinación del trabajo de la máquina no viniera impuesta por las conexiones externas de unas clavijas, sino por las órdenes almacenadas en la memoria eléctrica de la computadora.

I) La EDVAC (1949)

"El mismo que trabajó en la construcción de la ENIAC, Eckert y Mauchiy, construyó una segunda máquina, mayor que la ENIAC, con el nombre de EDVAC (Electronical Discrete Variable Automatic Computer), capaz de realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente".[17]

[16] Ibidem. p. 119.
[17] Ibidem. p. 120.

J) La UNIVAC (1951)

"La Compañía Remington Rand fundada por los mismos Éckert y Mauchly desarrolló la UNIVAC I (Universal Automatic Computer), que fue la primera computadora de uso comercial, y que apareció en 1951"[18].

Entre sus características principales encontramos el uso de cinta magnética para la entrada y salida de datos, la capacidad de aceptar y procesar datos alfabéticos y numéricos, así como el uso de un programa especial capaz de traducir programas en un lenguaje particular a lenguaje de máquina.

Estas máquinas constituyen la llamada primera generación de computadoras, que utilizaron bulbos de alto vacío como componentes básicos de sus circuitos internos. Como consecuencia, eran demasiado voluminosas, consumían mucha energía y producían calor; no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno pero limitado.

El siguiente avance tecnológico en la industria de las computadoras fue la sustitución de los bulbos por transistores que redujeron las deficiencias y mejoraron las ventajas ya existentes, introduciendo las memorias de ferrita que permitieron reducir el tamaño. Así surgió la segunda generación de computadoras.

En 1963 aparecen en el mercado las computadoras de la tercera generación, en las que encontramos como principal característica el uso de circuitos integrados monolíticos, que aumentaron considerablemente la velocidad de operación, incrementaron su confiabilidad y disminuyeron su costo y tamaño.

A partir de la tercera generación, los avances en la industria de la computación han sido tan numerosos y frecuentes que de alguna manera han hecho que el hombre de nuestro tiempo pierda su capacidad de asombro. Las

[18] Ibidem. p. 121.

computadoras han invadido la industria, el comercio, la administración, la educación y han llegado hasta nuestros hogares, constituyéndose esta industria en la segunda en importancia en el mundo, después de la automotriz.

Así, tenemos la llamada cuarta generación, con la integración a larga escala (LSI) y la aparición de microcircuitos integrados en plaquetas de silicio (chips) con notorias mejoras, en especial a nivel de la llamada microprogramación (firmware).

1.3 CLASIFICACIÓN DE LAS COMPUTADORAS.

Una de las clasificaciones más usuales de las computadoras tiene en cuenta la potencia o poder de cómputo. Como es de suponer, en esta clasificación intervienen factores como la longitud de palabra, la velocidad de funcionamiento, la capacidad de memoria y el número de terminales interactivos conectables. A continuación, mencionare los tipos de computadoras que considero de acuerdo a esta clasificación en orden decreciente de potencia. Como es lógico, dada la dificultad de llevar a cabo cualquier clasificación y la gran variedad de computadoras existentes, puede que las fronteras entre algunas de las categorías que aquí presento no estén lo suficientemente claras.

SUPERCOMPUTADORAS

Éste es el tipo de computadora más potente que existe, caracterizándose fundamentalmente por su gran rapidez y su gran longitud de palabra. La mayoría de las supercomputadoras disponen de varios procesadores trabajando en paralelo, consiguiendo velocidades del orden de billones de operaciones por segundo. Se utilizan para realizar cálculos complejos a gran velocidad sobre un gran volumen de datos (simulación de procesos complejos, como la fisión nuclear, la contaminación del aire de una ciudad, modelos atmosféricos para predicción meteorológica, etc.). Estas computadoras tan potentes generan una enorme cantidad de calor, que ha de ser disipado de alguna forma. Para solucionar este problema, los principales fabricantes de supercomputadoras toman determinadas

opciones para su diseño y construcción (Cray Research Inc usa enfriadores líquidos y diseños curvos para radiar el calor acumulado). Las supercomputadoras pueden costar de 10 a 30 millones de dólares, y tienen un altísimo consumo de energía eléctrica. Por ejemplo, CRAY Y-MP.[19]

MACROCOMPUTADORAS (MAINFRAMES)

"Son grandes computadoras de uso general con amplias posibilidades de procesamiento; memoria y E/S. Al igual que las supercomputadoras, requieren una instalación especial dentro de un entorno controlado y se utilizan para el procesamiento de grandes cantidades de datos en grandes empresas y organizaciones (bancos, compañías aéreas, agencias estatales, etc.). Su potencia de cálculo es inferior a la de una supercomputadora (varios millones de operaciones por segundo). Destacan por permitir utilización concurrente por gran número de usuarios conectados a través de terminales; estos usuarios se conectan a una mainframe para aprovechar su gran capacidad de almacenamiento masivo (donde se albergan grandes bases de datos centrales). Suelen costar entre 200.000 dólares y varios millones de dólares Por ejemplo, IBM/4361".[20]

MINICOMPUTADORAS

"Surgieron con la idea de disminuir los costes de las mainframes, aun a costa de sacrificar las prestaciones, ya que muchas organizaciones y compañías necesitan la potencia de una macrocomputadora, pero no pueden pagarla. Son similares a una mainframe, pero a escala reducida en precio y prestaciones (número de terminales y capacidad de disco). Estos equipos son utilizados por empresas de tipo medio y suelen costar entre 20.000 y 250.000 dólares. Por ejemplo, VAX de Digital Equipment Corporation (DEC)".[21]

---

[19] Ureña López, Alfonso. Fundamentos de la Informática. México 1999. Edit. Alfaomega. p. 14.
[20] Ibidem.
[21] Ibidem. p. 15.

ESTACIONES DE TRABAJO (WORKSTA TIONS)

"Se utilizan en forma monousuario y disponen de pantalla, ratón y teclado. Son microcomputadoras con potente CPU, que actúan conectados a redes para usar los recursos de ordenadores de mayor potencia. La principal diferencia entre una estación de trabajo y una computadora personal es que la primera esta basada en una filosofía de diseño de CPU, denominada RISC, que permite un procesamiento más rápido de las instrucciones. Por otro lado, las estaciones de trabajo suelen utilizar el sistema operativo UNIX y su uso se centra en aplicaciones científico-técnicas (ingeniería y gráficas). Por ejemplo, SUN SPARC".[22]

ORDENADORES PERSONALES (PC)

"Con este nombre se suele designar a la familia de microordenadores compatibles con el PC de IBM y la línea Macintosh de APPLE. Son microordenadores de fácil manejo que se suelen utilizar en forma monousuario. Suelen presentar unidades de disco flexible y disco rígido. Se caracterizan por su gran compatibilidad y bajo costo (entre 500 y 7.500 dólares), lo cual hace que la mayor gama de equipos hardware y de aplicaciones software que existen en el mercado se orienten a este grupo de computadoras. Existen versiones portátiles que permiten un fácil y cómodo transporte sin perder ninguna de las cualidades de un PC clásico".[23]

CALCULADORAS PROGRÁMABLES

"Se trata de un equipo de pequeño tamaño que funciona con pilas. Posee un teclado sencillo como unidad de entrada y un visualizador óptico como unidad de salida. Para programar estas máquinas se hace uso de un lenguaje simple y reducido, y la capacidad de memoria disponible suele ser bastante pequeña

[22] Ibidem.
[23] Ibidem.

(algunos Kbs)".[24]

1.4. APLICACIONES DE LA INFORMÁTICA

En los comienzos de la informática, debido al alto costo de las computadoras, estas máquinas sólo eran utilizadas por grandes instituciones (Departamento de Defensa de EEUU, instituciones gubernamentales, universidades, etc.) para realizar tareas numéricas complejas. No obstante, con el tiempo, el coste de los equipos ha ido disminuyendo continuamente y, de forma paralela, se han ido descubriendo nuevos usos de las computadoras. Hoy en día existen pocas actividades humanas en las cuales no tenga incidencia de forma directa o indirecta la informática.

A continuación cito algunas de las aplicaciones más importantes de la informática en la actualidad.

PROCESAMIENTO DE DATOS ADMINISTRATIVOS

Éste es el área de aplicación de mayor impacto; de hecho, sin computadoras, la economía se paralizaría por completo. En este campo se incluye todo lo relacionado con la automatización de las funciones típicas de gestión empresarial, como son la gestión de personal, proceso de nóminas y contabilidad, facturación, control de inventario, gestión bancaria, problemas de optimización, investigación de mercado, etc.

También dentro del ámbito administrativo han tenido gran importancia las aplicaciones relacionadas con la automatización del trabajo de oficina que han dado lugar a la aparición de una nueva técnica, la ofimática. Asociadas a la ofimática se encuentran las aplicaciones de tratamiento de textos, gestión de datos, hoja de cálculo, correo electrónico, agenda electrónica, desarrollo de presentaciones y otras aplicaciones relacionadas.

---

[24] Ibidem.

Por último, es necesario resaltar el gran desarrollo e importancia que están teniendo las aplicaciones de sistemas de información empresarial (Management Information System - MIS). Un MIS es un sistema o conjunto de reglas y procedimientos que proporcionan información fiable a las personas de una organización. Estos sistemas resultan imprescindibles en las empresas modernas y competitivas, ya que ayudan a la toma de decisiones a partir del análisis de todos los datos relacionados con el negocio.

APLICACIONES INDUSTRIALES Y DE INGENIERÍA

La computadora ha tenido también un importante papel como herramienta para facilitar los procesos de diseño y fabricación de productos. Dentro de este área, sus principales usos son trazado de planos, control de procesos industriales, rebotica industrial, minería, etc. También aquí se incluyen las aplicaciones de diseño asistido por computadora (Computer-Aied Design-CAD), fabricación asistida por computadora (Computer-Aided Manufacturing-CAM) y diseño, fabricación y prueba con ayuda de la computadora (Computer-Aided Design Manufacturing And Testing-CADMAT).

APLICACIONES TÉCNICO-CIENTÍFICAS

La computadora es utilizada ampliamente por los científicos como herramienta imprescindible en el campo de la investigación. cabe destacar el uso de las computadoras para acceder a grandes bases de datos distribuidas por diversos lugares, desarrollar teorías, recoger y validar datos. También aquí se incluyen todas las aplicaciones relativas al uso de la computadora para la resolución de modelos complejos (simulación, análisis de datos experimentales, etc.) y cálculos matemáticos (cálculo numérico, etc.), dentro de las cuales podemos citar: predicción meteorológica, control ambiental, control de tráfico, control de comunicaciones, control sísmico, etc.

APLICACIONES MÉDICAS Y BIOLÓGICAS

Actualmente, se utilizan las computadoras en todas las tareas médicas Se incluyen aplicaciones de investigación médica (biológica y farmacéutica). ayuda al diagnóstico y tratamiento de enfermedades, bases de datos de historiales clínicos de pacientes, control de pacientes en cuidados intensivos, ecografía, etc. Es esta una de la aplicaciones que mas adelante abordaremos de forma más detallada, por ser sumamente importante en el presente trabajo de investigación.

APLICACIONES MILITARES

El uso de la computadoras por parte de los gobiernos en aplicaciones militares ha precedido a las demás aplicaciones. De hecho, la primer computadora, la ENIAC. fue usada en un principio para calcular trayectorias balísticas ante diferentes condiciones, y el mayor consumidor de informática del mundo es el Departamento de Defensa de Estados Unidos. Dentro de este tipo de aplicaciones, destacan los sistemas computerizados de radar, los misiles autodirigidos, el espionaje militar por satélite artificial, los sistemas de seguridad y defensa computerizados, etc.

APLICACIONES EDUCATIVAS

En los últimos años, las computadoras personales han iniciado una revolución en el área educativa, individuos de todas las edades pueden utilizar las computadoras para conseguir un beneficio intelectual. Hoy en día, se pueden encontrar computadoras, en salones de clase, museos y bibliotecas. Además, la computadora se está convirtiendo en un instrumento esencial en el proceso de aprendizaje.

No obstante, el impacto de las computadoras en la educación puede ser contemplado desde dos puntos de vista. Por una parte, se plantea la necesidad de incluir la informática como materia en los planes de estudios, dada la importancia de que una persona este formada en el uso y aprovechamiento de la tecnología

computacional. Por otra parte, el ordenador (computadora) constituye un complemento muy útil en la formación del estudiante.

APLICACIONES EN EL ARTE Y HUMANIDADES

Aquí se incluyen aspectos relacionados con el arte. como son la composición de cuadros, creación de dibujos animados, música por computadora, industria cinematográfica. etc., así como el análisis automático de textos de cualquier naturaleza, etc.

OTROS CAMPOS DE APLICACIÓN

Entre las áreas de aplicación no englobadas en los puntos anteriores que merecen ser citadas se incluyen: prensa, ocio y entretenimiento (videojuegos), aplicaciones domésticas, seguridad y orden público, práctica legal (bases de datos jurídicas), sistemas de teletexto y videotexto, etc.

CAPÍTULO II.

PARTICULARIDADES DE INTERNET

Internet, con su variedad de tecnologías, ha sido promotor de cambio y principal constructor de una nueva sociedad global en la era digital. Gracias a este nuevo sistema de comunicación e información, cada una de las etapas comprendidas en los procesos básicos de las organizaciones, (creación, producción, comunicación, venta, servicio y control), pueden encontrar amplias posibilidades de proyección para resolver complejas operaciones de cualquier índole, simplificar o suprimir pasos innecesarios, detectar irregularidades, e inventar nuevas maneras de coordinar procesos, de un modo más ágil y efectivo, en busca de la innovación.

Así, después de exponer los aspectos generales de la computadora y la informática, corresponde ahora presentar los antecedentes y características generales de Internet.

2.1. DEFINICIÓN DE INTERNET

Hace algunos años ya existía Internet en México pero los usuarios mexicanos eran una minoría integrada por algunos estudiosos de la Informática. INTERNET confunde a muchos usuarios de computadora debido a sus diferencias con los programas de computo tradicionales. No es un programa, no es una pieza de hardware, no es software, ni siquiera es un sistema. Más bien es un lugar donde se puede obtener información, ponerla a disposición de los demás (en forma gratuita o por enajenación) y conocer servicios y gente.

En esencia, "INTERNET es una red de computadoras que ofrece acceso a gente e información. Más de diez millones de personas la utilizan y se espera que este número llegue a más de cien millones dentro de algunos años".[25]

[25] Hoffman, Paul. Internet. México 1998. Edit. Mc. Graw-Hill. p. ix.

Para usar Internet se ejecutan varios comandos desde su ordenador, dependiendo del tipo de información que desea . Por ejemplo puede utilizarse un programa para correo, otro para recuperar archivos y un tercero para participar en juegos con mucha gente a la vez y obtener un servicio o una publicación en INTERNET.

Internet es una gigantesca red de computadoras que va creciendo día con día, la información como ya se mencionó es muy variada, como pueden ser información científica, información comercial, bolsa de trabajo, video juegos, avisos de ocasión, investigaciones, deportes, ventas, programas administrativos y de negocios, cotizaciones, programas educativos, noticias y en fin una amplia gama de información que crece y se actualiza constantemente.

2.2. ANTECEDENTES HISTÓRICOS DE INTERNET

Internet fue creado por el Departamento de Defensa de los Estados Unidos para intercomunicar todas sus instalaciones. Posteriormente llego a las universidades de ese país y después experimento un crecimiento sin precedentes.

La creación de la red comenzó en 1969 cuando la agencia para Proyectos de Investigación Avanzada del departamento de Defensa contrató a la empresa Boll, Beranek and Newman para diseñar y desarrollar la red ARPANET, que en su nombre lleva las iniciales del organismo que lo ordeno según sus siglas en inglés. El objetivo de este sistema era conectar unas cuantas instituciones:

- El instituto de Investigación de Stanford
- La Universidad de Utah y las de California
- Puntos estratégicos en Los Ángeles y Santa Barbara

Estas instituciones realizan proyectos de desarrollo de armamento y sistemas de seguridad nacional para la Defensa estadounidense.

Esta red, denominada ARPAnet, tenía múltiples objetivos, que se

establecieron y son todavía parte de lo que hoy es Internet. Algunos de estos objetivos incluyen:

La red sería capaz de funcionar aun cuando muchas de sus computadoras o las conexiones entre ellas fallaran.

Para acomodar los diversos tipos de computadoras que entraban al mercado, el Departamento de Defensa quería que computadoras diferentes fueran capaces de intercambiar información sin problemas.. Así, el método del funcionamiento en red tenía que poder usarse en computadoras con configuraciones de hardware muy distintas.

La red sería capaz de redirigir la información de modo automático alrededor de sus partes que no estuvieran funcionando. Para hacer una comparación con un viaje por carretera, imágenes que va por la autopista de Nueva York a Bostón. Si su ruta planeada a través de Hartford estuviera bloqueada por una accidente, podría tomar el camino a través de Providence. Si estas dos rutas estuvieran intransitables, podría tomar una tercera a través de Albany. La red tendría que ser capaz de hacer este tipo de cambios de dirección automáticamente.

ARPAnet debía ser una red de redes, no únicamente de computadoras. Sólo una computadora de cada red tendría que conectarse directamente al hardware de ARPAnet. Parecería que todas las demás computadoras en esa red local estuvieran "en" ARPAnet y podrían comunicarse con otras computadoras también en ARPAnet a través de esta única conexión.[26]

La red tenía que estar diseñada para que en caso de un ataque nuclear nunca se interrumpiera la comunicación entre el Pentágono y los científicos que trabajan en los proyectos de defensa, pues era de vital importancia mantener la conexión en cuanto a los avances que se fueran suscitando y así poder seguir con los proyectos de prioridad.

---

[26] Hoffman, Paul. Internet, Manual de bolsillo. México 1995. Edit. Mc. Graw-Hill. pp. 3-4.

La confiabilidad de la red radicaba en que en caso de que alguno de los enlaces fuera interrumpido por un ataque militar, el tráfico de información se desviara automáticamente a otro "nodo".

Con el tiempo la red se fue desarrollando y se convirtió en un importante vehículo de comunicación para las universidades y centros de investigación que intercambiaban información y descubrimientos a través de ella, lo que atrajo a más y más instituciones relacionadas con la ciencia y las actividades académicas. Más adelante la red fue perfeccionada por el científico estadounidense Vinton Cerf en 1973 dentro del departamento de Defensa de Estados Unidos (Darpa) liderado por el ingeniero Robert Kahn. Para ello, se desarrolló el esquema técnico denominado protocolo Internet (IP conforme a sus siglas en inglés) que no solo mantenía comunicadas a las dos redes de Internet, sino que dirigía el tráfico de información de una a otra según fuera necesario. Es así que todos los sistemas conectados a ella permiten intercambiar mensajes entre sí.

Para principios de los años setenta, ARPANET contaba con cerca de medio centenar de "nodos" o centros conectados, cifra que al empezar los ochenta era alrededor de los 200.

Pero además de crecer, la red había cambiado especialmente en la forma en que se utilizaba. Ya no era un vehículo de intercambio de datos de investigación, ahora los usuarios se comunicaban entre ellos a través de buzones privados de correo electrónico.

A partir de 1980, la computación en las universidades aumentó de un número pequeño de máquinas compartidas, cada una de ellas con cientos de usuarios simultáneos, a un gran número de pequeñas estaciones de trabajo para escritorio. Pero los usuarios se habían acostumbrado a las ventajas de los sistemas compartidos, como los directorios y el correo electrónico y deseaban mantener esas ventajas en sus estaciones de trabajo.

En 1983 ARPANET se dividió en dos: la red militar MILNET y en una

ARPANET o red pública más pequeña, el término Internet se utilizó para conocer al conjunto de los dos sistemas.

Aun cuando esa época solo existían dos redes, IP fue diseñado para permitir que decenas de miles de redes de trabajo estuvieran comunicadas. Un hecho especial de este protocolo es que en principio todas las computadoras de la red son tan capaces como cualquier otra por lo que todas las máquinas pueden comunicarse sin importar sus diferencias técnicas.

Un año después, en 1984 cuando muchos expertos sitúan el nacimiento de Internet, La National Science Foundation (Agencia Nacional para la Ciencia, otro organismo gubernamental estadounidense) fundó la NSFNET. Esta red había creado cinco centros de super-computadoras para que sus servicios pudieran ser accesibles a cualquier institución educativa.

Estos centros otorgaron al mundo académico acceso a los sistemas informáticos más veloces en todo el orbe, tan caros que sólo se construyeron cinco.

Al principio, estos centros de supercomputación iban a ser instalados como parte de ARPANET, pero hubo muchos problemas, tanto técnicos como políticos que lo impidieron, por lo cual se decidió crear NSFNET. Más tarde, la fundación estableció un puñado de redes para conectar a los usuarios de cada zona del país tanto estatales como regionales.

NSFNET funcionaba tan bien que a principios de los 90s muchos negocios se habían cambiado de ARPANET a NSFNET, ya que la red del Pentágono, tras 20 años de servicio, resultaba obsoleta. Fue por esa razón que la cancelaron. Sin embargo, los centros de supercomputadoras que soportaba NSFNET no resultaron ser tan exitosos: algunas de las costosas máquinas no funcionaban y las que si servían eran tan caras que la mayoría de los usuarios empezaron a buscar equipos más sencillos, pero con alta capacidad de desempeño. Esto permitió el desarrollo tecnológico que llevó al crecimiento y popularidad de

Internet, la cual se limitó a la conexión de redes pequeñas entre sí.

La NSFNET no desapareció, todavía existe pero permite sólo el tráfico relacionado con la investigación y la educación.

En 1991, el entonces senador Al Gore decidió que si Estados Unidos quería continuar a la cabeza del llamado "primer mundo" tenía que dar más importancia a la computación y a las redes. Para ello, patrocinó el Congreso "Computación de Alto Rendimiento" en 1991, de la cual salió la Red para la Investigación y Educación Nacional (NREN conforme a sus siglas en inglés).

La NSFNET se convirtió en la "espina dorsal" de Internet y el punto de partida del crecimiento de la hoy llamada "Supercarretera" de la información.

Actualmente, el núcleo de la red se encuentra en Estados Unidos y funciona desde 1992. Dado que el tráfico en Internet crece día con día, se tiene ya planeado incrementar los enlaces y se trabaja en ampliar su capacidad de manejo de la información.

Hoy en día, Estados Unidos tiene la mayor penetración de usuarios Internet. Singapur, un país característicamente cerrado y controlado, ocupa la segunda posición, debido a que su gobierno busca convertir a esa nación en un centro de comercio mundial.

La red permite que 146 países envíen y reciban todo tipo de correo electrónico.

En cuanto a las redes conectadas a Internet, 636,000 se encuentran en instituciones educativas y más de 550,000 han sido registradas como usuarios comerciales. Son precisamente ellos quienes tienen el crecimiento más acelerado, con 92% anual.

2.3. HISTORIA DE INTERNET EN MÉXICO

En México se creó la red MEXNET constituida por enlaces que comunican a los nodos del Instituto Politécnico Nacional, en el D.F.; la Universidad de Guadalajara, en Jalisco; la Universidad de las Américas, en Puebla y el Instituto Tecnológico de Estudios Superiores de Monterrey.

El otro gigante de Internet en el país, orgullosamente es la Universidad Nacional Autónoma de México (UNAM) tiene una conexión directa con la red regional del sureste de Estados Unidos.

La historia de la entrada de la UNAM a la red empezó en 1989 cuando entraron a la red BITNET que funcionaba en la red de la Fundación Nacional para la Ciencia de Estados Unidos.

Esto permitió que para 1990 empezara el funcionamiento de Internet en México, con lo cual lo primero que se habilitó fue el correo electrónico, las listas de discusión y los FTP o transferencia gratuita de archivos y programas de un lado a otro.

Dos años después, en 1992 se incorporó el popular sistema de búsqueda Gopher y para el 93 se habían desarrollado las bases de datos más importantes y las primeras revistas electrónicas.

En 1994 se crearon en la UNAM los servicios hemerográficos y se empezaron a ofrecer servicios de periódicos y textos completos de libros. En ese mismo año empezó a funcionar el servidor de búsqueda por palabra Verónica.

El año antepasado, la UNAM inició el trabajo con el World Wide Web, que es un sistema de búsqueda de información en la red sencillo y accesible así como las videoconferencias, es decir, transmisión de voz e imagen entre puntos distantes, pero a tiempo real. Cabe señalar que la red ha crecido enormemente, no sólo en México sino en todo el mundo.

2.4. FUNCIONAMIENTO DE INTERNET

Internet ha sido por mucho tiempo una red internacional, pero sólo se había extendido hacia los países que mantenían buenas relaciones diplomáticas con Estados Unidos y a las bases militares de este país ubicadas fuera de su territorio.

Hoy en día, Internet se ha esparcido por todos lados, se encuentra en más de 60 países y el número crece rápidamente. Las naciones de Europa Oriental con lazos científicos con Occidente han querido participar desde mucho tiempo atrás, pero fueron excluidos por las regulaciones del gobierno. Como el bloque de los países ex socialistas. Los países del tercer mundo que anteriormente no contaban con los recursos para participar en la red la ven ahora como un medio para elevar sus niveles educativos y tecnológicos.

Cuando se trata de imaginar qué es Internet y cómo opera, lo normal es pensar en un sistema telefónico. Después de todo, ambos son electrónicos y permiten abrir una conexión y transferir información. Internet está compuesta principalmente por líneas telefónicas permanentemente dedicadas a este uso.

La red telefónica es una red de conmutación de circuitos. Cuando se llama por teléfono se separa de una parte de la red; por ejemplo, cuando la línea está en espera esta es inaccesible para otras personas, lo que causa una subutilización de un recurso muy costoso: la red.

El Protocolo Internet (IP) se hace cargo de establecer domicilios o se asegura de que los enrutadores sepan qué hacer con la información que les llega. Una parte de la información del domicilio figura al principio del mensaje.

El domicilio está compuesto por varias partes. Como Internet es una red de redes, los primeros números del domicilio indican a los enrutadores cuál es la red a la que usted pertenece. Los últimos indican qué computadora personal o equipo anfitrión de la red debe recibir el paquete. Bajo este esquema, cada computadora en Internet tiene un domicilio único.

La supercarretera de la información no es más que otra expresión de la vida humana, con sus fortalezas y sus debilidades.

"Internet posibilita a quien tiene acceso, y sepa manejarlo, alcanzar muchísimas fuentes de información no manipuladas por ningún gobierno o grupo de interés. Uno puede conseguir los datos y discriminar entre los que son falsos y los que son ciertos; puede ir a los sitios desde donde se distribuye la información y ponerse en contacto con las persona que la generan para cuestionarlas de manera personal y directa, cosa imposible cuando se trata de la televisión, la radio e incluso los periódicos".[27]

Hay quienes la llaman la red de redes, otros la súper carretera de la información y otros simplemente la Web; no importa cómo la nombren, lo sorprendente son los alcances que desprende y la movilidad que el usuario puede alcanzar con su poderoso dedo índice y sólo dando un clic al ratón.

Las repercusiones de Internet en la vida cotidiana se disparan en un infinito abanico de opciones para cada caso, la era Internet es un agente de cambio en la manera en que vivimos, trabajamos, aprendemos y jugamos. Han surgido nuevos verbos como "chatear" y hay un importante glosario a considera con términos tecnológicos y otros creados por los mismos usuarios, formando así un nuevo caló informático digno de ser analizado por la Real Academia de la Lengua Española.

Por otra parte, existe la llamada "Economía de Internet", herramienta práctica y estratégica para los negocios que está transformando a todas las empresas tanto públicas como privadas, ya que les permite tener ventajas competitivas al ofrecer información crítica a clientes, socios de negocio, empleados y proveedores durante las 24 horas del día y los siete días de la semana, además de mantener interacción con su entorno.

---

[27] Rozenberg, Dino. "La nueva cultura de la información", citado en Revista Expansión, mayo 1998. p. 28.

Las empresas de la nueva economía, o e-economy de Internet están utilizando a la red par mejorar la productividad, reducir el tiempo de venta, incrementar utilidades y construir relaciones de todo tipo. En cualquier economía de mercado, las reglas del juego definen quién gana y quién pierde entre países, negocios y personas. Quienes se adapten a la nueva economía de Internet tendrán todas las ventajas de la globalizaciones.

La maravilla del Internet en los negocios reside en su rentabilidad: a mayor producción, mayores ganancias; crecimiento, más transacciones en menos tiempo y competitividad.

Los clientes virtuales son cada vez más exigentes en cuanto al servicio y a la puntualidad de sus entregas sin que por ello vean demeritada la calidad del producto. Actualmente Internet implica cambios de hábitos de consumo mediante el comercio electrónico. Esto no quiere decir que vamos a dejar de consumir, sólo vamos a dejar de consumir, sólo va a cambiar la forma de hacerlo y los clientes serán más exigentes.

CAPÍTULO III.

TRANSGRESIONES A TERCEROS POR MEDIO DE LA INFORMÁTICA.

Hay personas que consideran que los delitos informáticos, como tales, no existen. Argumentan que tan sólo son delitos normales que en lo único que se pueden diferenciar, de otro delito cualquiera, son en las herramientas empleadas o en los objetos sobre los que se producen.

Creo que ésta es una visión demasiado limitada de la realidad: Esto puede ser así si pensamos tan solo en delitos del tipo de un apunte informático falso en un banco o del robo de una cantidad de dinero gracias a la utilización ilícita de una tarjeta de crédito.

Pero existen muchos otros delitos que difícilmente podemos tipificar con las leyes actuales y que estas rápidamente se tendrán que adaptar o redactar acorde a los nuevos tiempos, que impone el uso de las tecnologías de la información. Por ello, se habla constantemente de lagunas o de falta de regulación.

Un ejemplo clarificador es lo que ocurrió con el famoso gusano de Internet, que lanzó Robert Morris Jr. en Noviembre de 1988 y que acabó bloqueando más de 6000 computadoras: De no existir en ese momento el Acta sobre Fraude y Abuso Informático en Estados Unidos, es más que dudoso que se le hubiese podido juzgar.

Hay que recordar también que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido.

También hay que recordar "que hasta la propia Dirección General de Policía en algunos países como España, ha tenido que crear un grupo dedicado en exclusiva a los delitos informáticos.

Casi el 90% de los delitos informáticos que investiga el FBI tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos?

La solución pasa por una coordinación internacional, tanto al investigar como al aplicar leyes que deben contar con un núcleo común. Es decir, hay que unificar criterios: difícil será actuar contra un delito que si lo es en un país y no en otro. En este sentido está trabajando, por ejemplo, la Unión Europea.

Además el avance que está sufriendo Internet en número de usuarios, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella: con el aumento de la ciberpoblación, aumentan los posibles delincuentes y los posibles objetivos.

Mucha empresas que en un principio no querían conectarse a Internet, precisamente por los posibles problemas de seguridad, ahora no quieren quedarse atrás, ya que se ha convertido en una cuestión o de pura necesidad o de imagen, y ahora se conectan a marchas forzadas, lo que hace que muchas no tomen las precauciones necesarias y se conviertan automáticamente en jugosos y fáciles objetivos.

Internet no estaba pensada y desarrollada para lo que está ocurriendo: su propio diseño no está basado sobre protocolos hiper-seguros y, tan es así, que hoy día se estima que no existe un sólo servidor en el mundo que no haya sufrido un ataque contra su seguridad por parte de hackers y crackers.

Desde el punto de vista de la seguridad también es preocupante el uso de la criptología por parte de los delincuentes, tanto para ocultar sus mensajes haciéndolos ininteligibles, como para ocultar sus propios movimientos en un sistema informático, haciendo que incluso aunque sean detectados no se pueda saber exactamente que es lo que estaban haciendo, al estar encriptados los archivos descubiertos. En este sentido, actualmente es muy inquietante la

utilización de cripto-virus (programas con código vírico encriptados).

Lógicamente, no es que la criptología sea mala en si (presenta más ventajas que desventajas): el problema surge cuando es utilizada por malas manos.

3.1. CONCEPTO DE "DELITOS INFORMÁTICOS"

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, etcétera. 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.

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

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".[28]

De esta forma, conceptualiza al delito informático en forma típica y atípica,

[28] Téllez Valdes, Julio. Derecho Informático. México 1996. Edit. Mc. Graw-Hill. p. 103.

entendiendo por la primera a " las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador"[29]

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".[30]

El delito informático se considera, entonces como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos.

María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[31]

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

---

[29] Ibidem. p. 104.
[30] Callegari, Nidia. "Delitos Informáticos y Legislación" Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín Colombia 1985. p. 115.
[31] Lima De, Luz María. "Delitos Informáticos" en Criminalia. México 1984. Academia Mexicana de Ciencias Penales. Edit. Porrua. No. 1-6. Año L. p. 100.

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como recurso para evitar su impunidad.

No más de 10% de los crímenes de alta tecnología son reportados y de ellos sólo se investigan 3%. Es decir, menos de la mitad de estos ilícitos son llevados a proceso. Si fueras un cibercriminal, las posibilidades de ser capturado, procesado y mandado a prisión son muy remotas por el momento, aunque las condiciones están cambiando.

3.2. TIPOS DE DELITOS INFORMÁTICOS

Los tipos de delitos informáticos reconocidos por Naciones Unidas son:

Fraudes cometidos mediante manipulación de computadoras.

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.

La 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.

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.

Fraude efectuado por manipulación informática

Aprovecha las 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.

Falsificaciones informáticas.

Como objeto:

Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos:

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, 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.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático:

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus:

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y 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.

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.

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.

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.

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.

Los piratas informáticos pueden provocar 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 moderna. Al respecto, considero, 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.

3.3. HACKERS Y CRACKERS

Cuando se produce un delito informático, en muchas de las ocasiones, suelen aparecer los hackers como el centro de atención, tanto de rebote como por ser efectivamente los responsables del supuesto penal del que se trate. Es conveniente hacer referencia de manera particular a los siguientes conceptos:

Hacker. Sería el curioso, el que simplemente le gusta meterse a husmear por todas partes, llegar a comprender el funcionamiento de cualquier sistema informático mejor que quienes lo inventaron.

El término es objeto de continuo debate entre el mismo movimiento, pero la definición más concisa, por lo que se puede deducir, radica en que un hacker sería aquel amante de la informática, con grandes conocimientos de la materia (programación, sistemas, redes, criptografía, etc.), que se siente parte de un movimiento contracultural positivo para que la información sea libre, al igual que el acceso a la misma, y que lidian contra la tentación de grandes compañías, instituciones públicas y demás, que pretenden controlar esta información. Son, de alguna forma, los últimos románticos con un gran arma en sus manos: la computadora.

Toma su actividad como un reto intelectual, no pretende producir daños e, incluso, se apoya en un código ético:

- El acceso a los ordenadores, y a cualquier cosa que te pueda enseñar cómo funciona el mundo, debería ser ilimitado y total.
- Toda la información debería ser libre y gratuita.
- Desconfía de la autoridad. Promueve la descentralización.
- Los hackers deberían ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza o posición social.

- Se puede crear arte y belleza en un ordenador. (Aquí se incluye tanto la belleza en su sentido tradicional, como la belleza que puede tener un código fuente bien escrito).

- Los ordenadores pueden mejorar tu vida.

- Se le puede llegar a reprochar que esta visión romántica cada vez se ajusta menos a la realidad, que hay una finísima línea entre actuar así y producir un desaguisado (aunque sea involuntariamente) o caer en la tentación de robar información. Por no hablar que en numerosas legislaciones, el mero hecho de colarse en un sistema (aunque sólo sea eso) ya es delito. En muchas ocasiones, aunque su intención sea únicamente curiosear, las consecuencias de los métodos que utilicen, por ejemplo el empleo de (royanos, hacen que deriven importantes consecuencias económicas, ya que el administrador del sistema que descubra este tipo de cosas desconoce las intenciones reales del intruso, y suelen ser importantes los perjuicios ocasionados en tiempo y recursos empleados para limpiar el sistema. De todas formas es injusto que, gracias a la prensa menos informada o a películas sensacionalistas, automáticamente se equipare este término al de pirata informático.

- Cracker. Realmente es a esta clase de personaje al que nos estamos refiriendo cuando hablamos de pirata informático. Presenta principalmente dos vertientes:

- El que se cuela en un sistema informático y roba información o produce destrozos en el mismo.

- El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti-copia.

- Phreaker. Es el especialista en telefonía. Se le podría llamar el cracker de los teléfonos. Sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. ¡Ni que decir tienel que están muy perseguidos, por la Justicia y por las compañías telefónicas.

3.3.1. VÍCTIMAS DE LOS HACKERS Y LOS CRACKERS.

Todos los usuarios de computadoras (ordenadores) son victimas potenciales de los hackers y los crackers, ya que no solo estan expuestos a contagiar su equipo de algun virus sino tambien existen grandes posibilidades que al estar conectados a la red (Internet) alguno o algunos de los sujetos antes mencionados logre "hackear" la computadora provocando algun daño a la información contenida en el equipo e incluso en el mismo.

A continuación mencionare algunos de los casos mas sonados de crimen por computadora.

- Austin Ron y Kevin Poulsen.

En 1982 dos hackers de los Angeles, Ron Austin y Kevin Poulsen, se introdujeron en la red de intercambio de datos Arpa del Pentágono, la precursora de la actual Internet. La primera opción, en el esquema virtual que poseían, era adivinar la palabra clave de acceso al sistema. Lo lograron al cuarto intento, utilizando las letras UCB, las iniciales de la Universidad de California, en Berkeley. Estos saqueadores, aumentaron la capacidad del usuario ordinario UCB, diseñando una subrutina para "captar" los privilegios del superusuario "Jim Miller". Su "ciberpaseo" terminó al intentar hojear unos ficheros "cebo", preparados para mantener el mayor tiempo posible conectados a los hackers, pero no sin antes sacar algo de provecho: el manual de Unix, el sistema operativo multitarea, diseñado por los laboratorios Bell (organismo de investigación de la ATT) la mayor compra a telefónica de EE.UU.

- Gates, Bill y Allen, Paul.

En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Grandes programadores. Empezaron en los 80 y han creado el mayor imperio de software de todo el mundo. Sus "éxitos" incluyen el SO MS-DOS, Windows, Windows 95 y Windows NT.

- Draper, John. Captain Crunch.

En septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch duplica perfectamente la frecuencia de tono de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT&T.

- Holland, Wau y Wenery, Steffen.

De visita en la NASA "Las dos de la madrugada, Hannover, ciudad Alemana, estaba en silencio. La primavera llegaba a su fin, y dentro del cuarto cerrado el calor ahogaba. Hacía rato que Wau Holland y Steffen Wernery permanecían sentados frente a la pantalla de una computadora, casi inmóviles, inmersos en una nube de humo cambiando ideas en susurros.

Cuando la computadora comenzó a ronronear, Wau Holland y Steffen Wernery supieron que habían logrado su objetivo. Segundos más tarde la pantalla mostraba un mensaje: "Bienvenidos a las instalaciones VAX del cuartel genera, de la NASA". Wau sintió un sacudón y atinó a escribir en su cuaderno: "Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad".

El 2 de mayo de 1987, los dos hackers alemanes, de 23 y 20 años respectivamente, ingresaron sin autorización al sistema de la central de investigaciones aerospaciales.

- Ing-Hou, Chen.

Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los

que llamo "proveedores incompetentes de antivirus para software", dijo la policía ahora. Pero él admitió que no esperaba que CIH causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo. El virus Chernobyl — conocido en Taiwan como el CIH, por las iniciales de Chen — fue mostrado a la Armada China de Liberación para que lo estudiaran. Para la prevención de la invasión de las computadoras. Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico. Chen desde su egreso ha estado bajo el mandato de Taiwan a dos años de servicio militar.

Este inusual virus destructivo — programado para funcionar el 26 de Abril, osea el 13 aniversario del desastre nuclear de Chernobyl, trata de borrar el disco duro de la computadora y escribir garabatos dentro del sistema para que no arranque la máquina.

- Kevin & Ronald, Makaveli & Tooshort.

Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 98, a la edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa. Simplemente fueron formados por algún "experto hacker", que se encontraba a miles de kilómetros de su pueblo natal, Cloverdale, y que se hacía llamar el "Pirata Maestro".

- Levin, Vladimir.

Un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street, Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin

espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.

- Mentor, El, H4G13.

Casi todo es posible dentro de la imaginación de los hackers. Un grupo de estos delincuentes, a los que algunos llaman corsarios, denominado H4G13, consiguió romper los códigos de seguridad de la NASA. Simplemente querían demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, dejando las cosas bien claras, colocando en la pagina principal de la NASA, durante media hora, un "manifiesto"

- Mitnick Kevin, "El Cóndor", "El Chacal de la red".

Como Hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar". Su bautizo como infractor de la ley fue en 1981. Junto a dos amigos entró físicamente a las oficinas de COSMOS de Pacific Bell. COSMOS (Computer System for Mainframe Operations) era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas. Una vez dentro de las oficinas obtuvieron la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS. La información robada tenía un valor equivalente a los 200 mil dólares. Fueron delatados por la novia de uno de los amigos y debido a su minoría de edad una Corte Juvenil lo sentenció a tres meses de cárcel y a un año bajo libertad condicional.

Luego de cumplido el período de tres meses el oficial custodio encargado de su caso encontró que su teléfono fue desconectado y que en la compañía telefónica no había ningún registro de él.

Sus objetivos iban creciendo a cada paso y en 1982 entró ilegalmente, vía módem, a la computadora del North American Air Defense Command en Colorado. Antes de entrar alteró el programa encargado de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar. El FBI, creyendo que había hallado a Mitnick, allanó la casa de unos inmigrantes que estaban viendo televisión.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de accesar a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador.

Para 1991 ya era el Hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue

invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Allanaron su casa pero había desaparecido sin dejar rastro alguno. Ahora Mitnick se había convertido en un Hacker prófugo.

También en 1992, el Departamento de Vehículos de California ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick por haber tratado de obtener una licencia de conducir de manera fraudulenta, utilizando un código de acceso y enviando sus datos vía fax.

En la Navidad de 1994, invadió la computadora de Tsutomu Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen Hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros Hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al Hacker que había invadido su privacidad.

Hacia finales de enero de 1995, el software de Shimomura fue hallado en una cuenta en The Well, un proveedor de Internet en California. Mitnick había creado una cuenta fantasma en ese proveedor y desde allí utilizaba las herramientas de Shimomura para lanzar ataques hacia una docena de corporaciones de computadoras, entre ellas Motorola, Apple y Qualcomm.

Shimomura se reunió con el gerente de The Well y con un técnico de Sprint (proveedor de servicios telefónicos celulares) y descubrieron que Mitnick había creado un número celular fantasma para accesar el sistema. Luego de dos semanas de rastreos determinaron que las llamadas provenían de Raleigh, California.

Shimomura se comunicó con el FBI y éstos enviaron a un grupo de rastreo por radio. El equipo de rastreo poseía un simulador de celda, un equipo normalmente utilizado para probar teléfonos celulares pero modificado para rastrear el telefono de Mitnick mientras este está encendido y aunque no esté en uso. Con este aparato el celular se convertiría en un transmisor sin que el usuario lo supiera.

A medianoche terminaron de colocar los equipos en una Van y comenzó la búsqueda de la señal, porque eso era lo que querían localizar; no buscaban a un hombre porque todas las fotos que tenían eran viejas y no estaban seguros de su aspecto actual, el objetivo de esa noche era determinar el lugar de procedencia de la señal. Ya para la madrugada localizaron la señal en un grupo de apartamentos pero no pudieron determinar en cuál debido a interferencias en la señal.

Mitnick también es sospechoso de robar el software que las compañías telefónicas piensan usar para todo tipo de procesos, desde la facturación hasta el seguimiento del origen de una llamada pasando por la decodificación de las señales de los teléfonos celulares para preservar su privacidad.

Según el Departamento de Justicia de los Estados Unidos, este "terrorista electrónico", conocido como "el Cóndor", fue capaz de crear números telefónicos imposibles de facturar, de apropiarse de 20.000 números de tarjetas de crédito de habitantes de California y de burlarse del FBI por varios años.

Kevin Mitnick. Este sencillo nombre, oculta la verdadera identidad de uno de los mayores hackers de la historia. Fue una de las mayores pesadillas del

Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles y llegó a falsificar 20.000 números de tarjetas de crédito.

Al igual que el chico de la película "Juegos de Guerra", Mitnik se introdujo en el ordenador de la Comandancia para la Defensa de Norte América, en Colorado Springs.

Pero a diferencia del muchacho de Juegos de Guerra, Mitnik se dedicó a destruir y alterar datos, incluyendo las fichas del encargado de vigilar su libertad condicional y las de otros enemigos. La compañía Digital Equipment afirmó que las incursiones de Mitnik le costaron más de cuatro millones de dólares que se fueron en la reconstrucción de los archivos y las pérdidas ocasionadas por el tiempo que los ordenadores estuvieron fuera de servicio.

Lunes, 22 de marzo de 1999. REDACCIÓN.

El hacker más famoso del mundo, Kevin Mitnick, que dio lugar al guión de la película "Juegos de Guerra" y lleva en prisión desde 1995, ha conseguido un acuerdo con jueces y fiscales en vísperas del inicio de la vista, fijada para el 29 de marzo. Los términos concretos del acuerdo se desconocen, pues ninguna de las partes ha efectuado declaraciones, pero según informó, el jueves 18, "Los Ángeles Times", Mitnick, de 35 años, podría quedar en libertad dentro de un año, aunque tendría prohibido durante tres años más el acceso a ordenadores y, además, se le vetaría que obtuviera rendimiento económico contando su historia en medios de comunicación.

Sobre él pesaba una condena de 25 años por fraude informático y posesión ilegal de archivos sustraídos de compañías como Motorola y Sun Microsystems.

Estando en libertad provisional, en 1992, realizó diversas acciones de "hacking", y permaneció como fugitivo hasta su captura, en Carolina del Norte, en 1995.

Encarcelado por el Gobierno norteamericano sin juicio, Kevin Mitnick había sido considerado por el FBI como el hacker más peligroso y escurridizo del mundo.

- Morris Robert.

En noviembre de 1988, Morris lanzo un programa "gusano" diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares. Se creo el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.

- Murphy Ian, Captain Zap.

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap,". Mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los

accesos restringidos a compañías electrónicas, y tenía acceso a órdenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados" explico Murphy. "El violar accesos nos resultaba muy divertido".

- Paint & Hagis,

Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores mas utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", ¡accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante: "¡Todos los que el mes pasado utilizaron el motor de búsqueda Yahoo! han adquirido una bomba lógica que se activará el día de Navidad, sembrando el caos en todas las redes informáticas del planeta". Y añadían que solo entregarán el antídoto del virus si Mitnick, condenado a 35 años de prisión, quedaba en libertad. La bomba no pasó de ser una amenaza, pero el efecto de llamar la atención sobre el caso Mitnick se había conseguido.

Si cumplían con sus requisitos, el programa antídoto, oculto en un ordenador, sería suministrado a los cibernautas. Todo se quedó en palabras, porque según la portavoz de Yahoo, Diane Hunt, los hackers accedieron a la página de la empresa, pero no destruyeron ni infectaron nada.

- Poulsen Kevin, Dark Dante.

Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de "Dark Dante" en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.

- Smith, David.

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear las comunicaciones publicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta diez años de cárcel.

- Zinn, Herbert, Shadowhack.

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenía entre 16 y 17 años cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y una fianza de US $10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US $800,000 si hubiera tenido 18 años al momento del crimen.

CASOS ANÓNIMOS SONADOS DE CRIMEN POR COMPUTADORA.

En 1988, varios hackers consiguieron entrar en los ordenadores de siete universidades de Gran Bretaña, la de Londres incluida. Para resolver este crimen, la policía necesito la ayuda técnica de un asesor informático, Robert Jones. Una vez arrestado un sospechoso, las pruebas se analizaron durante un año y medio antes de presentarlas ante el tribunal, que lo condeno a un año de prisión. Después de varias colaboraciones más, Scotland Yard propuso la creación de un centro universitario dedicado a la investigación de estos casos. El Centro de Investigación de Delitos Informáticos, adscrito al Queen Mary & Westfield College, se creó a principios de 1996 y el abogado Ian Walden, experto en la legislación de

tecnología de la información, es su director. El Centro obtiene fondos del Gobierno y se dedica a la investigación y la asesoría en el campo de los delitos informáticos, así como a impartir cursos de formación en la materia para policías, fiscales, abogados y cualquier interesado.[32]

En 1989 la justicia alemana detiene a un grupo de crackers germanos que habían copiado durante años miles de programas de acceso no legal y passwords de ordenadores en departamentos de la administración de EEUU. El destinatario de la información era el KGB soviético.

También en 1993 la compañía discográfica Frank music Corporation vence en su demanda contra Compuserve, el mayor proveedor de Internet, por permitir que sus abonados copiaran más de 500 canciones sometidas a derechos de autor. Otras 140 discográficas han denunciado a Compuserve por idéntica razón.

En 1993 la revista Play Boy gana un juicio contra George Frena, que había distribuido ilegalmente en su BBS fotos de desnudos procedentes del web de esta publicación. En 1993 y 1994, Play Boy denunció a 12 BBS más por el mismo motivo.

El 19 de Septiembre de 1996, la CIA sufrió los ataques de un grupo de Hackers suecos, que desmantelaron su servidor de Información en Internet, modificando el mensaje de presentación "Bienvenidos a la Agencia Central de Inteligencia" por "Bienvenidos a la Agencia Central de Estupidez". Entre la maraña de contenidos de la Web, colocaron también varias conexiones directas a otros lugares de Internet, como a las revistas Flashback o Playboy. La CIA experimentó una grave derrota, con lo que tuvo que retirar su maltrecho servidor.[33]

En Mayo de 1997, un grupo de hackers ("cortadores") asalta la página de una de las películas más taquilleras de la fábrica Spilberg: Jurassic Park,

[32] Klander, Lars. A prueba de hackers. Argentina 1998. Edit. Anaya Multimedia. p. 19.
[33] Ibidem.

cambiando durante 18 horas el logotipo del dinosaurio por otro en el que aparecía un pato.

Nadie está fuera del alcance de estos saqueadores, ni siquiera el todopoderoso Bill Gates, que vio cómo la Homepage de Microsoft fue atacada por varios hackers en junio de 1997. Estos hackers, accedieron al sistema operativo por un bug de Windows Nt 4.0, el cual era el servidor bajo el que se ejecutaba la Web de Microsoft. Hay muchas formas de dar publicidad a actos "presumiblemente ilegales", pero algunas son más ingeniosas que otras.[34]

Una de las hazañas más sorprendentes de intercambio de información entre hackers fue el caso Price. En esta ocasión, se investigó la acción de un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde allí conseguía entrar en los ordenadores del Ministerio de Defensa de los Estados Unidos. Llegó a copiar archivos que no eran materia reservada, pero sí investigaciones de temas delicados. Su centro de trabajo era su casa, en Londres, y desde allí causó uno de los mayores desastres informáticos de la década. No trabajaba solo, por lo que intercambió todos los documentos que había obtenido con hackers de distintos países, vía Internet. El caos fue total, llegando incluso al cierre temporal de la red norteamericana.[35]

Pero lo que más sorprende al mundo del underground, y más aún, a los ciudadanos de a pie es que, estos asaltos, en más de una ocasión, no son perpetrados por "gurús" de la informática, ni por miembros de la "elite hacker" sino más bien por principiantes, por iniciados al hacking.

Microsoft ha anunciado firmes avances en su lucha contra el delito informático durante el año fiscal de 1997, que incluye el embargo de cerca de 100,000 copias ilegales o programas falsos, CD-ROM y dispositivos hardware,

[34] Ibidem. p. 20.
[35] Ibidem. p. 22.

procedentes de canales de distribución europeos y con un valor de más de 23 millones de dólares.

ESTE ES UN RESUMEN DE LOS ACTOS DE "CIBERVANDALISMO"MÁS CONOCIDO EN EL CIBERESPACIO

Pagina	Hacker	Fecha	Información acerca:
Tolla	The Kevin Mitnick Liberation Front	3/17/96	La compañía más grande de telecomunicaciones e Internet fue hackeada por segunda vez en el mismo día, después de asegurar en radio nacional la imposible de violar la seguridad. Piden la liberación de Kevin Mitnick.
Department of Justice	???	8/18/96	Hackeada como protesta contra la proposición de censar el Internet y hacer ilegal transmitir pornografía en la red.
CIA	Power Through Resistance	9/20/96	¡Este sitio hizo noticia en el CNN!. El Fiscal Sueco, Bo Skarinder, proceso la semana anterior a 5 personas por hackear. Modificaron la página y pusieron: "Bienvenidos a la Agencia Central de Estupidez"
Kriegsman	The Ghost Shirt Factory	11/12/96	Una fabrica que vende abrigos de pieles fue hackeada por un activista de los derechos de los animales, colocando vínculos a paginas a favor de la fauna.
Nothosting	01001000 00110111	11/27/96	Nethosting tiene su pagina electrónica y todos sus las paginas de sus 1500 clientes fueron hackeadas en un día, solo para darse a conocer.
Labour	???	12/12/96	El partido británico del trabajo fue hackeado. "Misma política, mismas mentiras". Además de declaraciones en contra de los políticos.
NASA	\\StOrM\\	12/23/96	El encabezado de la pagina decía "La NASA patrocina a los hackers". Además de críticas, vínculos a playboy y otras paginas.
NASA	\\StOrM\\	12/30/96	De nuevo una semana después. "No emociona explorar el Challenger.."
U.S. Air force	???	12/30/96	El título de la página fue "Bienvenidos a la verdad", además se colocaron críticas contra el gobierno e imágenes fuertes.
Employment Network	???	1/8/97	Se colocaron críticas al gobierno, y esta pagina se mantuvo por casi una semana.
Republic of Indonesia	TOXYN	2/11/97	La página del Dpto. de Asuntos exteriores de Indonesia fue hackeada. Esto fue hecho para protestar contra la ocupación de Indonesia en el East Timor.
NASA	H4G1S	3/5/97	Críticas al gobierno EUA. Además de comentarios a favor de la liberación de Kevin Mitnick y Ed Cummings
Cyber promotions	???	3/19/97	"¡Finalmente! La página de Cyberpromotions del gordo cerdo Sanford Wallace's fue hackeada. Este es el tipo que llena tu buzón con basura y hace dinero por eso". .

Amnesty International	4 man dream team	4/26/97	Amnistía Internacional fue hackeada, "¿Quien ríe al ultimo?".
Conservativo	Circle of Deception	4/27/97	El partido Conservador británico fue hackeado, "ahora tienen, por lo menos algo en común con el partido del trabajo".
Jurassic Park	hackers(?)	5/27/97	La pagina "El Mundo Perdido" fue hackeada 4 días después del estreno de la película, duró 12 horas con una figura parecida a un pato.
LAPD	P.A.R.A.	5/29/97	"Bienvenidos a la página de LADP, el escuadrón de la muerte", siendo encabezado de una foto de la golpiza a Rodney King.
Geocities	fr0llc	6/25/97	La página principal de Geocities fue hackeada.
C.S.I.S.	???	7/15/97	¡¡El servicio canadiense de seguridad fue hackeado!!
Crack Mac	Starfire	8/18/97	"Gran concurso para hackear la página".
Value Jet	???	10/1/97	"¡Vuela con nosotros, porque estrellarse es divertido!".
Pentagon	Chameleon	10/4/97	El Centro Armado de Inteligencia Artificial de EUA fue hackeado.
Whitepower	L.O.U.	10/11/97	Esta pagina a favor del poder blanco fue "cómicamente" hackeada.
Spice Girls	Team CodeZero	11/14/97	La página oficial de las Spice Girls fue hackeada, y fuertes criticas fueron publicadas con referencia a la calidad del grupo.
China Agricultural University	LSD	11/26/97	Esta página fue hackeada con criticas en contra de la ocupación del Tibet por China. Y en contra de la prueba de armas nucleares.
Yahoo	PANTZ/ H4GiS	12/8/97	Este popular buscador fue hackeado durante alrededor de 15 minutos, y solo fue visto por algunas personas. "Liberen Kevin Mitnick".
FOX	???	12/11/97	El canal de TV FOX, fue hackeado. (Son los únicos que pasan los Expedientes X en USA). Así se mantuvo mucho tiempo.
China Agricultural University	W1n{} Dose & 1-s-d	12/31/97	El mismo servidor Chino fue hackeado. "¿Por qué EUA comercializa con China y no con Cuba?, Saquen a esa gente del Tibet".
Janet Jackson	Team CodeZero	1/2/98	La página oficial de Janet Jackson. Modificaron la apariencia de la pagina al cambiar la foto.
Rolling Stones	Team CodeZero	1/2/98	Página oficial de los Rolling Stones, se une a las Spice Girls, Janet Jackon, La Red de Defensa de Sistemas de Información de EUA, etc.
BMW	???	1/2/98	La página de los automóviles alemanes fue hackeada.
UNICEF	D.A.M.M.	1/7/98	El UNICEF fue hackeado. "Liberen a Kevin Mitnick".

Indonesia	LithiumError/ ChiKo-Torremendez	1/18/98	"Bienvenido a lo cruel, violento y corrupto". Cerca de 15 paginas de Indonesia fueron hackeadas al mismo tiempo. Esto como parte de la anticampaña a Suharto (para presidente).
International Church of Christ	???	1/18/98	Página de la Iglesia Internacional de Cristo, modificada, con criticas en contra. "Vida eterna a cambio de todo tu dinero, si, nosotros lo prometemos".
legislate	No|d Crew	1/21/98	"Buenas declaraciones" (www.legislate.com).
Saatchi& Saatchi	Trix&Vertex	2/19/98	Saatchi&Saatchi, fueron premiados por innovaciones en comunicación.
One Live Crew	???	2/22/98	Página en protesta sobre el abuso sexual a infantes.
Universidad Turca	Gr Power	3/5/98	En protesta a la presencia turca en Chipre..
NAMBLA	74074	3/6/98	En protesta al abuso a menores, NAMBLA.
US Army	No|d Crew	3/8/98	Ya van 3 páginas de diferentes servidores de los EUA que son hackeadas.
US Navy	No|d Crew	3/9/98	La página del Comando del Espacio Naval fue hackeada. Criticas al gobierno.
Korean Heritage College	RaPtoR 666	4/14/98	La página de "The Korean Heritage College of North America" fue hackeada.
Leonardo DiCaprio	D3str0, Fouk0, Lunat1c	4/19/98	La página de oficial del actor Leonardo DiCaprio's fue ecomicamente modificada, alterando la fotografia de inicio.
Motorola	H4CK1NG F0R G1RL13Z	8/21/98	Motorola fue hackeada 2 veces el mismo día. Una fue a la división de semiconductores y la otra fue la pagina principal de Motorola Japonesa. El seudónimo utilizado es "Hackeando por mujeres".
Arsenal F.C.	Cumbrian Alliance	8/30/98	La pagina oficial del Club de Football Arsenal Football fue hackeada en protesta por la expulsión del entrenador.
New York Times	H4CK1NG F0R G1RL13Z	9/12/98	Otro golpe de "Hackeando por mujeres". En protesta a las declaraciones hechas por un reportero en relación a Kevin Mitnick.
Id Software	rd	9/24/98	id Software's, fue hackeada. La pagina fue modificada muchas veces. Pero no estuvo disponible por mucho tiempo.
SCO	ax	11/7/98	SCO (Santa Cruz Corporation) tiene muchos servidores hackeados en diferentes paises. SCO's sitio Mexicano en http://www.sco.com.mx.
Jack Daniels	FLUXX	12/14/98	La página de Jack Daniels fue hackeada.
Calgary Public	the leprechaun	1/25/99	La biblioteca publica fue hackeada como medio para comunicar la opresión en el norte de

Library			Irlanda. Sin tener relación con el hecho.
Greenpeace	???	1/27/99(?)	La página de la asociación internacional Greenpeace fue hackeada. Liberen a Kevin Mitnick.
Front National	RaPtoR 666	1/28/99	El partido Fascista francés "Front National" fue hackeado.
200 Cigarettes	MagicFX	2/20/99	Película de Hollywood hackeada.
Dominos Pizza	Cyrus	2/28/99	Dominos Pizza fue hackeada. "Yo charlo en irc"..
Monica Lewinsky	Magic FX	3/5/99	Mónica Lewinsky.com fue hackeada. Y modificaron la pagina.
Pussy-Power	???	3/5/99	Mas acerca de Mónica Lewinsky.
Ministerio Griego de Asuntos Exteriores	Kalamata Hacking	3/23/99	Página del Ministerio de asuntos exteriores en Gracia. Fue hackeado en protesta por los asuntos relacionados con el asentamiento turco, el gobierno, además del crimen.
Hot Bot	???	3/25/99	HotBot, una de los 5 mejores motores de búsqueda fue hackeado, colocando su autor un mensaje relacionado con la falta de raíces en las culturas y la influencia de los EU en eso.
Playboy Sprint Yellowpages Sony Music	???	4/4/99	Muchas paginas han sido hackeadas y remplazadas por la misma pagina electrónica. También, la página de Bárbara Streisand, Oreilly.com, Umd.edu, hornyrob.com, sun.ca, y muchas otras.

3.3.2. CONSECUENCIAS MÉDICAS.

Como sabemos cualquier usuario de equipos de cómputo puede ser víctima de los hackers y los crackers ahora bien, una de las victimas que considero sería interesante analizar son las instituciones dedicadas a los estudios e investigaciones de las ciencias médicas, ya que las computadoras se utilizan en todas las tareas médicas Se incluyen aplicaciones de investigación médica (biológica y farmacéutica). Ayuda al diagnóstico y tratamiento de enfermedades, bases de datos de historiales clínicos de pacientes, control de pacientes en cuidados intensivos, ecografía, etc.

En el subcapitulo anterior fue posible analizar lo perjudicial que puede ser que un equipo de cómputo sea hackeado o infectado por un virus informático, también se pudo observar que aun los sistemas más sofisticados son vulnerables

y los daños sufridos son de una gran magnitud.

Por lo anterior podemos inferir que la perdida o modificación de la información contenida en las computadoras de instituciones de estudios e investigación médica traería como consecuencia desde errores en análisis realizados a pacientes, esto va de la mano con diagnósticos erróneos que podrían provocar hasta la muerte del paciente, otro problema que puede presentarse es el al estar desarrollando la cura o tratamiento de alguna enfermedad, se llegue a perder información sumamente valiosa, información que talvez llevo muchos años conseguir y que muy probablemente sea materialmente imposible recuperar.

Las anteriores son algunas de las consecuencias que es menester evitar a cualquier costo, por ser de vital importancia para el ser humano.

3.3.3. DETECCIÓN DE LA PROBLEMÁTICA EN EL EQUIPO DE COMPUTO.

A continuación analizaremos como se pueden detectar los problemas en el equipo de cómputo una vez que fueron contagiados por un virus adquirido vía Internet o por algún disquete infectado.

Realmente nadie puede determinar a ciencia cierta qué síntomas muestra el sistema cuando está infectado ya que los virus son muy variados y sus formas de comportamiento también, a esto se suma que en la actualidad los virus bien programados son mucho más sofisticados que antes y reconocer la presencia de un virus con un simple vistazo no es una habilidad que muchos puedan ostentar.

Podemos mencionar algunos indicios que delatarían la presencia de un virus pero la lista no es definitiva:

- Los comandos o acciones que hacemos ejecutar por la computadora aparentan ser más lentos. Esto es debido a que hay un programita extra que no está en nuestros cálculos y que trabaja sobre cada una de las cosas que nosotros hacemos. De todas formas resulta un poco

improbable ya que el tamaño de los virus, por lo general, no da lugar a que realicen extensas ejecuciones, descontando obviamente la lentitud de cualquier dispositivo periférico.

- Las aplicaciones que ya de por sí son un tanto pesadas en cargarse; resultan aún más debido a que existe un virus que provoca que la carga sea aun más lenta.

- Dispositivos como la HDD o la FDD son leídos repentinamente sin causa o motivo. Esto puede pasar cuando un virus intenta propagarse a un disquete, por ejemplo.

- Los archivos se incrementan levemente en tamaño. Puede ser a causa de un virus que parasita a esos archivos agregando su código al código ejecutable del archivo. En la actualidad resulta más difícil detectar un virus de estos ya que las técnicas stealth permiten que el virus manipule el tamaño de archivo que el usuario termina viendo en la pantalla. El resultado es que el usuario termina viendo el tamaño que tenía el archivo antes de ser infectado en vez del tamaño real actual.

- Programas o procesos en memoria que son desconocidos. Para un usuario experimentado resultaría extraño ver en memoria un proceso que él no autorizó a que sea cargado. Los sistemas operativos poseen distintos comandos o programas que permiten ver el estado de la memoria y poder determinar que programas se encuentran cargados en ese momento, entre otras cosas como la dirección en donde están localizados, el tamaño que ocupan, etc.

Existen otras manifestaciones que muchos confunden con síntomas cuando en realidad no lo son. Gráficos poco comunes que aparecen en la pantalla, mensajes nunca antes vistos, letras que se caen y rebotan en el fondo de la pantalla y todo otro tipo de cosas similar no son más que el accionar propio del virus. Los virus fueron programados para ese tipo de cosas (por más ridículas que

parezcan para algunos) y no son consecuencias secundarias en el sistema debido a que exista un virus.

Síntomas más comunes de virus:

Incluso el mejor software antivirus puede fallar a la hora de detectar un virus. La educación del personal sobre cuáles son posibles síntomas de virus informáticos puede ser la diferencia entre un simple dolor de cabeza y un gran problema. Veamos algunos síntomas:

- Los programas comienzan a ocupar más espacio de lo habitual.
- Aparecen o desaparecen archivos.
- Cambia el tamaño de un programa o un objeto.
- Aparecen mensajes u objetos extraños en la pantalla.
- El disco trabaja más de lo necesario.
- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados.
- La cantidad de espacio libre del disco disminuye sin ningún tipo de explicación.
- Se modifican sin razón aparente el nombre de los ficheros.
- No se puede acceder al disco duro.

El detectar un virus es reconocer la presencia de un accionar virósico en el sistema de acuerdo a las características de los tipos de virus. Identificar un virus es poder reconocer qué virus es de entre un montón de otros virus cargados en nuestra base de datos. Al identificarlo sabremos exactamente qué es lo que hace, haciendo inminente su eliminación.

Identificar un virus supone, primero, lograr su detección y luego poder determinar de qué virus se trata exactamente. A esta técnica se la conoce con el nombre de scanning o escaneo. Es muy sencilla de entender. El programa antivirus posee una base de datos con ciertas strings propias de cada virus, estas strings son cadenas de caracteres que el scanner del antivirus utilizará como huella digital para identificar de qué virus se trata, el scanner comienza a revisar uno por uno el código de los archivos almacenados intentando encontrar alguno de estos fragmentos representativos de los virus que tiene registrados. Con cada una de las verificaciones no se revisa la base de datos completa ya que resultaría bastante laborioso y una pérdida de tiempo considerable, aunque de hecho el hacer un escaneo de nuestra unidad de disco rígido lleva algún tiempo. Entonces, cada antivirus utilizará diferentes técnicas algoritmicas para agilizar un poco este paso de comparar el código contra su base de datos.

La técnica de scanning no resulta ser la solución definitiva, ni tampoco la más eficiente, pero continúa siendo la más utilizada debido a que permite identificar con cierta rapidez los virus más conocidos, que en definitiva son los que lograron adquirir mayor dispersión.

Teniendo en cuenta los puntos débiles de la técnica de scanning surgió la necesidad de incorporar otros métodos que complementaran al primero. Como ya se mencionó la detección consiste en reconocer el accionar de un virus por los conocimientos sobre comportamiento que se tienen sobre ellos, sin importar demasiado su identificación exacta. Este otro método buscará código que intente modificar la información de áreas sensibles del sistema sobre las cuales el usuario convencional no tiene control (y a veces ni siquiera tiene conocimiento), como el master boot record, el boot sector, la FAT, entre las más conocidas.

Otra forma de detección que podemos mencionar adopta, más bien, una posición de vigilancia constante y pasiva. Esta, monitorea cada una de las actividades que se realizan intentando determinar cuándo una de éstas intenta modificar sectores críticos de las unidades de almacenamiento (mencionados en

el primer párrafo de este apartado), entre otros. A esta técnica se la conoce como chequear la integridad.

ANÁLISIS HEURÍSTICO

La técnica de detección más común es la de análisis heurístico, consiste en buscar en el código de cada uno de los archivos cualquier que sea potencialmente dañina, acción típica de los virus informáticos, es una solución interesante tanto para virus conocidos como para los que no los son. El inconveniente es que muchas veces se nos presentarán falsas alarmas, cosas que el scanner heurístico considera peligrosas y que en realidad no lo son tanto. Por ejemplo: tal vez el programa revise el código del comando DEL (usado para borrar archivos) de MS-DOS y determine que puede ser un virus, cosa que en la realidad resulta bastante improbable. Este tipo de cosas hace que el usuario deba tener algunos conocimientos precisos sobre su sistema, con el fin de poder distinguir entre una falsa alarma y una detección real.

DEFINICIONES DE ANTIVIRUS

Los archivos de definiciones antivirus son fundamentales para que el método de identificación sea efectivo. Los virus que alcanzaron una considerable dispersión pueden llegar a ser analizados por los ingenieros especialistas en virus de algunas de las compañías antivirus, que mantendrán actualizadas las definiciones permitiendo así que las medidas de protección avancen casi al mismo paso en que lo hacen los virus.

Un antivirus que esté desactualizado puede resultar poco útil en sistemas que corren el riesgo de recibir ataques de virus nuevos (como organismos gubernamentales o empresas de tecnología de punta), y están reduciendo en un porcentaje bastante alto la posibilidad de protección. La actualización también puede venir por dos lados: actualizar el programa completo o actualizar las definiciones antivirus. Si contamos con un antivirus que posea técnicas de detección avanzadas, posibilidad de análisis heurístico, protección residente en

memoria de cualquiera de las partes sensibles de una unidad de almacenamiento, verificador de integridad, etc., estaremos bien protegidos para empezar. Una actualización del programa sería realmente justificable en caso de que incorpore algún nuevo método que realmente influye en la erradicación contra los virus. Sería importante también analizar el impacto económico que conllevará para nuestra empresa, ya que sería totalmente inútil tener el mejor antivirus y preocuparse por actualizar sus definiciones día por medio si nuestra red ni siquiera tiene acceso a Internet, tampoco acceso remoto de usuarios y el único intercambio de información es entre empleados que trabajan con un paquete de aplicaciones de oficina sin ningún contenido de macros o programación que de lugar a posibles infecciones.

3.4. CRIPTOLOGÍA

Se entiende por criptología el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.

La criptografía es la parte de la criptología que estudia como cifrar efectivamente los mensajes.

Esto que así dicho parece no revestir mayor importancia, se ha convertido en pieza clave de un debate que ha desbordado muchos foros restringidos, hasta configurarse como uno de los focos de mayor atención de la mayoría de los gobiernos del planeta: En algunos países está directamente prohibido el uso de mensajes cifrados (como Francia o China, por ejemplo), en otros como Estados Unidos está fuertemente controlado, impidiéndose la exportación de programas cifradores al considerarse por el Acta de Control de Exportación de Armas (Arms Export Control Act).

Hay muchos países que, aunque en su territorio nacional permiten el uso de la criptología, desean que estos programas incluyan una puerta trasera (backdoor) o procedimiento parecido para poder intervenir el mensaje cuando así lo

consideren oportuno: Es el caso del famoso chip de depósito de claves o Chip Clipper, para cifrar conversaciones telefónicas (los dos teléfonos participantes en una conversación deben tenerlo).

Todo esto nos lleva directamente al enfrentamiento de la privacidad en las comunicaciones-control gubernamental, lo que en términos orwellianos se denomina "el control del Gran Hermano" (aunque esta expresión se utiliza, también, para denominar a esa especie de ojo vigilante, que presuntamente nos acecha continuamente y cuyo origen es indeterminado: Gobiernos, espías de distinto grado, fisgones o meros curiosos...).

Lo cual desemboca en la posible afectación de derechos fundamentales de las personas, como es el derecho a la Libertad de Expresión, que difícilmente se puede conseguir si cuando nos comunicamos con alguien no sabemos quien o quienes pueden realmente leer el mensaje, y el Derecho a la Privacidad. Problema que se agrava en Internet, ya que los mensajes se pueden quedar en el ciberespacio por tiempo indefinido, sin tener nosotros siquiera consciencia de ello o de donde estará efectivamente copiada o almacenada nuestra comunicación.

La cuestión es conseguir que aunque nuestros mensajes puedan ser interceptados, resulten totalmente ininteligibles. Y esto se consigue con la criptología.

No estamos ante un problema trivial: es de vital importancia para que se desarrolle el comercio seguro en Internet, para los grupos defensores de los Derechos Humanos o para las comunicaciones entre abogados y sus clientes, por indicar algunos de los cientos de ejemplos posibles.

Para encriptar y desencriptar la información se utilizan llaves, que básicamente son combinaciones numéricas. Mientras más grande es la llave, más difícil es romperla para ver la información original. Grandes o pequeñas, las llaves se remiten a operaciones matemáticas, más o menos complejas: cuanto más complejas, ocuparán más memoria informática (o bites).

consideren oportuno: Es el caso del famoso chip de depósito de claves o Chip Clipper, para cifrar conversaciones telefónicas (los dos teléfonos participantes en una conversación deben tenerlo).

Todo esto nos lleva directamente al enfrentamiento de la privacidad en las comunicaciones-control gubernamental, lo que en términos orwellianos se denomina "el control del Gran Hermano" (aunque esta expresión se utiliza, también, para denominar a esa especie de ojo vigilante, que presuntamente nos acecha continuamente y cuyo origen es indeterminado: Gobiernos, espías de distinto grado, fisgones o meros curiosos...).

Lo cual desemboca en la posible afectación de derechos fundamentales de las personas, como es el derecho a la Libertad de Expresión, que difícilmente se puede conseguir si cuando nos comunicamos con alguien no sabemos quien o quienes pueden realmente leer el mensaje, y el Derecho a la Privacidad. Problema que se agrava en Internet, ya que los mensajes se pueden quedar en el ciberespacio por tiempo indefinido, sin tener nosotros siquiera consciencia de ello o de donde estará efectivamente copiada o almacenada nuestra comunicación.

La cuestión es conseguir que aunque nuestros mensajes puedan ser interceptados, resulten totalmente ininteligibles. Y esto se consigue con la criptología.

No estamos ante un problema trivial: es de vital importancia para que se desarrolle el comercio seguro en Internet, para los grupos defensores de los Derechos Humanos o para las comunicaciones entre abogados y sus clientes, por indicar algunos de los cientos de ejemplos posibles.

Para encriptar y desencriptar la información se utilizan llaves, que básicamente son combinaciones numéricas. Mientras más grande es la llave, más difícil es romperla para ver la información original. Grandes o pequeñas, las llaves se remiten a operaciones matemáticas, más o menos complejas: cuanto más complejas, ocuparán más memoria informática (o bites).

Existen dos tipos de llaves:

- Llaves simétricas: Se trata de un número o combinación de números que comunica al emisor que envía la información con el receptor autorizado par abrirla. Se enfocan a la confidencialidad. Generalmente ocupan 128 bites, pero el gobierno de Estados Unidos sólo permite la exportación de llaves simétricas de hasta 56 bites.

- Llaves asimétricas: Se conforman de dos números, uno público y otro privado. Generalmente se utilizan más en la firma digital. Ocupan unos 1024 bites o más; el gobierno de Estados Unidos sólo permite la exportación de llaves asimétricas de hasta 512 bites.

La mayoría de las veces se usan, de manera combinada, ambos tipos de llaves. Los términos básicos que se utilizan son los siguientes:

- Algoritmo. Es lo que se emplea para cifrar un mensaje (o lo que sea), resultando un código incomprensible que sólo se puede llegar a entender si se sabe como se ha cifrado.

- Clave secreta. Es el código básico utilizado para cifrar y descifrar un mensaje. Cuando se utiliza la misma para las dos funciones estamos ante un sistema simétrico.

- Clave pública. Es la clave que hacemos que esté al alcance de todo el mundo para que nos puedan enviar un mensaje cifrado. También con ella pueden descifrar lo que les enviemos cifrado con nuestra clave privada.

- Clave privada. Es la clave que tan sólo nosotros conocemos y que utilizamos para descifrar el mensaje que nos envían cifrado con nuestra clave pública. Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

La tendencia de los sistemas de clave simétrica, actualmente, es a utilizarlos poco o simplemente para cuestiones que no necesiten un alto grado de protección.

Los sistemas de clave asimétrica son los que se están imponiendo, ya que ofrecen un mayor grado de seguridad. Sobre todo porque no hace falta que la clave sea conocida nada más que por una persona. Ya se sabe que cuando un secreto se comparte, hay bastantes posibilidades para que deje de serlo.

Entre los programas cifradores de esta segunda clase, el que se está configurando como un standard (por lo menos en cuanto a los usuarios comentes) y goza de mayor popularidad es el PGP o Pretty Good Privacy (Privacidad Bastante Buena) de Phil Zimmermann, basado en un sistema de doble clave (una pública y otra privada). Existe tanto en versiones gratuitas como comerciales.

Aunque éste no es el único, la idea no es llenar la investigación de conceptos técnicos, si no simplemente indicar cual es el panorama del cifrado y, sobre todo, fijarnos en los problemas legales que plantea.

En España por ser un país con una legislación adecuada, no existen problemas al respecto, pero en muchos paises la situación legal está todavía por definir.

La colisión de intereses que se produce es, por un lado el Derecho a la Intimidad y a la Privacidad, y por otro, el deseo de los Cuerpos de Seguridad de que no exista información a la que no puedan tener acceso. Se promete interesante el debate en muchos países, como el que hay actualmente abierto en Estados Unidos: Por un lado los defensores de la Privacidad, por otro, cifras como las que presenta el FBI (y eso que ellos no llevan a cabo la totalidad de las escuchas realizadas en los EE.UU.):

Entre 1985 y 1994, las escuchas ordenadas judicialmente formaron parte de las pruebas que concluyeron en 14648 sentencias, supusieron casi 600

millones de dólares en multas y más de 1500 millones de dólares en recuperaciones y embargos ordenados por los jueces. Esto se imposibilitaría con el uso de cifrado fuerte.

Estados Unidos sigue una política de control de la exportación de criptografía, que podemos concretar en los siguientes puntos:

- Limitar la disponibilidad para los extranjeros de sistemas criptográficos estratégicamente capaces, concretamente, aquellos sistemas capaces de resistir un ataque criptoanalítico concertado.

- Limitar la disponibilidad para los extranjeros de sistemas criptográficos de fuerza suficiente para presentar una barrera seria a la selección de tráfico o el desarrollo de estándares que interfieran con la selección de tráfico, haciendo los mensajes en amplias clases de tráfico difíciles de distinguir.

Usar el proceso de control de la exportación como un mecanismo para seguir la pista de criptosistemas producidos comercialmente, tanto en los EE.UU. como extranjeros, que la Agencia de Seguridad Nacional (NSA) algún día tenga que romper.

3.5. ORGANISMOS INTERNACIONALES QUE HAN CREADO SISTEMAS DE PREVENCIÓN

El objetivo de este subcapítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de que contribuyan al desarrollo de este trabajo.

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los

derechos penales nacionales.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .... y en particular las directrices para los legisladores nacionales. Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, considero que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal (hasta ese entonces) era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias

desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados. internacionales de extradición.

Teniendo presente esa situación, considero que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas

afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

CAPÍTULO IV

CONTROL EN MÉXICO DE DELITOS INFORMÁTICOS.

Para el desarrollo de este capítulo se analizará la legislación nacional e internacional que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, en el caso de México aún no contemplan en sí los delitos informáticos. También será analizado dogmáticamente el delito de daño en propiedad ajena y como se comete vía internet.

4.1. CONCEPTO DE DAÑO EN PROPIEDAD AJENA.

Concepto

El delito de daño en propiedad ajena se encuentra previsto en el Código Penal Federal en el apartado de los delitos cometidos contra el patrimonio de las personas.

El tipo genérico está previsto en el artículo 399:

Cuando por cualquier medio se cause daño, destrucción o deterioro de cosa ajena, o de propia en perjuicio de tercero, se aplicarán las sanciones del robo simple.

El tipo específico está contemplado en el artículo 397:

Se impondrán de 5 a 10 años de prisión y multa de cien a cinco mil pesos a los que causen incendio, inundación o explosión con daño o peligro de:

I. Un edificio, vivienda o cuarto donde se encuentre alguna persona.

II. Ropas, muebles u objetos de tal forma que puedan causar daños personales.

III. Archivos públicos o notariales;

IV. Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos, y

V. Montes, bosques, selvas, pastos, mieses o cultivos de cualquier género.

Muchos autores han criticado el termino de daño en propiedad ajena, ya que este delito no solo puede recaer en cosas ajenas. A continuación daremos cuenta de algunos conceptos de diversos autores.

Francesco Carrara, menciona que es "un delito bárbaro en el que se destruye una cosa útil sin ninguna ventaja". Es decir que el sujeto que comete el delito no obtiene ningún beneficio, y este pude ser motivado por el odio, venganza y en algunos casos hasta ignora quien es el propietario del bien que esta dañando.

Mariano Jiménez Huerta, afirma que el termino de "Daño en propiedad ajena" es impropio además de que no coincide con su contenido ya que "la figura típica puede tener por objeto material, como expresa el artículo 399. la destrucción o deterioro de cosa propia en perjuicio de tercero".[36] Por tal motivo será más adecuada la denominación de "Delito de Daños".

Por su parte Francisco González de la Vega, apunta que el delito de daños "consiste en la destrucción o la inhabilitación totales o parciales de cosas corporales ajenas o propias con perjuicio o peligro de otro". [37] Menciona que la denominación adecuada al tipo debe ser la de delito de daño en las cosas.

El maestro Francisco Muñoz Conde, define el delito en estudio como delito de daños el cual según el maestro es aquel que "supone, en definitiva, que se quite o disminuya su valor a la cosa dañada, lesionando su esencia o sustancia".[38]

---

[36] Jiménez Huerta, Mariano. Derecho penal mexicano IV. México 1984. Edit. Porrúa. p. 407.
[37] González de la Vega, Francisco. Derecho penal mexicano. México 1990. Edit. Porrúa. p. 301.
[38] Muñoz Conde, Francisco. Derecho penal. Parte especial. 1985. Edit. Publicaciones de la universidad de sevilla. pp. 320 y 321.

Según Eduardo López Betancourt, el delito de daño en propiedad ajena es "la afectación o lesión de bienes jurídicamente tutelados, originados por un agente externo viable, sea directa o indirectamente."[39]

En lo personal considero que el termino adecuado es el de daños, el cual podría definirse como: la destrucción, deterioro o menoscabo de una cosa, que le quite o disminuya su valor, ya sea de cambio o de uso en perjuicio de un tercero.

Enseguida será realizado un breve estudio dogmático del delito en referencia.

I.- Clasificación del delito.

Es un delito:

- Por la conducta: de acción u omisión.
- Por el número de actos: unisubsistente o plurisubsistente.
- Por el resultado: de lesión o peligro.
- Por el daño: de resultado material.
- Por su duración: instantáneo o continuado.
- Por el número de sujetos: unisujetivo.
- Por ordenación metodológica: fundamental básico y especial.
- Por su autonomía: autónomo o independiente.
- Por su composición: anormal.

II.- Imputabilidad e Inimputabilidad.

[39] López Betancourt, Eduardo. Delitos en particular I. México 1994. Edit. Porrúa. p. 379.

- Imputabilidad:

En el campo del Derecho Penal el sujeto es imputable cuando se cumplan dos condiciones:

1.- Ser mayor de edad.

2.- Estar en pleno uso de las facultades.

En el primer supuesto se discute si el sujeto hasta los dieciocho años tendrá capacidad y conocimiento de sus actos.

En el segundo supuesto se requiere que el individuo además de ser mayor de dieciocho años no padezca alguna enfermedad mental, es decir este en pleno uso de sus facultades mentales.

- Inimputabilidad:

Se presenta cuando al realizar el hecho típico, el agente no tiene capacidad de comprender el carácter ilícito de aquel o conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo mental retardado.

La inimputablidad abarca a los menores de edad y enfermos mentales.

Si el agente se provocó el trastorno mental dolosa o culposamente, será responsable por el resultado, siempre y cuando lo haya previsto o le fuere previsible; doctrinalmente se conoce como "acciones libres en su causa".

III.- Conducta y su ausencia.

- Conducta:

a) Clasificación:

1.- De acción: Se presenta mediante movimientos corporales encaminados a producir el hecho delictivo.

2.- De comisión por omisión: Se presenta cuando el agente deja de hacer lo que debe, produciéndose el hecho delictivo.

b) Sujetos:

1.- Activo: Es quien realiza la conducta u omisión que produce el daño, deterioro o destrucción de la cosa ajena o propia en perjuicio de tercero. Puede ser cualquier persona.

2.- Pasivo: Es sobre quien recae el daño patrimonial.

c) Objetos:

1.- Material: Es el daño producido en la cosa en si.

2.- Jurídico: Es el daño producido en el patrimonio.

d) Medios de comisión: Se da mediante el tipo genérico, no exige ningún medio comisivo.

- Ausencia de conducta:

a) Fuerza mayor.

b) Fuerza física.

c) Movimientos reflejos.

d) Hipnotismo.

e) Sonambulismo.

IV.- Tipicidad y Atipicidad:

Tipicidad:

Existe cuando se presentan todos los elementos del tipo que describen al

delito.

- Sujeto (Activo y Pasivo).
- Conducta Típica.
- Medios de comisión.
- Resultado típico.
- Objetos material y jurídico.

Atipicidad:

Se da cuando falta alguno de los elementos antes mencionados.

V.- Antijuridicidad y Causas de Justificación.

Antijuridicidad:

El daño en propiedad ajena es antijurídico, pues la ley tutela el patrimonio de las personas por medio de ese tipo.

Causas de Justificación:

a) Estado de necesidad.

b) Cumplimiento de un deber.

c) Ejercicio de un derecho.

VI.- Culpabilidad e Inculpabilidad.

Culpabilidad:

a) Dolo.- Este delito se puede cometer en forma dolosa, es decir con intención de cometer un ilícito.

b) Culpa.- Este delito también puede darse por culpa, cuando el agente no tiene intención de cometer el ilicito, se puede presentar por negligencia, imprudencia, o impericia.

Inculpabilidad:

a) Error esencial de hecho invencible: El sujeto piensa que está actuando bajo alguna causa de justificación.

b) No exigibilidad de otra conducta: Se presenta cuando no se puede exigir por parte del sujeto activo otra conducta diferente a la que realizo.

c) Caso fortuito: Es cuando existe un verdadero accidente.

VII.- Punibilidad y Excusas Absolutorias.

Punibilidad:

Es el merecimiento de la pena, el artículo 397 contempla una pena de 5 a 10 años de prisión y multa de cien a cinco mil pesos; el artículo 399 indica que se castigará con las sanciones del robo simple.

Excusas absolutorias:

En el delito en estudio no existen.

Una vez que fue analizado minuciosamente el delito de daño en propiedad ajena, cabe mencionar que algunos autores han denominado como sabotaje informático a este delito cuando es cometido para dañar computadoras o programas informáticos, a continuación mencionare algunas definiciones de diversos autores.

La palabra Sabotaje viene del francés Sabots, que eran unos pequeños zapatos de madera que utilizaban los hijos de los obreros en las grandes fábricas industriales francesas, y que eran utilizados para trabar las máquinas en dichas

fábricas, con el fin de protestar por el despido de sus padres y las malas condiciones laborales. Para el diccionario de la Real Academia de la Lengua Española, sabotaje, es la "acción u omisión consistente en dañar ciertas instalaciones, productos, servicios públicos, y en general los bienes sociales, económicos y militares, realizada por los obreros en apoyo de sus reivindicaciones o por los enemigos de un régimen político".

El sabotaje informático consiste en la destrucción o inutilización del soporte lógico, esto es, de datos y/o programas contenidos en un ordenador (en sus bandas magnéticas).

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema informático, o telemático.

Considero personalmente que el término sabotaje no es el apropiado para definir dichas conductas, por cuanto dicha expresión tiene connotaciones políticas y sociales intrinsecas en su significado y que no siempre estarán presentes en el agente al cometer el acto ilicito, por tal razón considero que sería mas adecuado hablar de Daños Informáticos, pero dado que la doctrina unánimemente se ha pronunciado por usar dicho término diremos que el Sabotaje Informático es: el conjunto de conductas maliciosas, que utilizando cualquier método o modo destruyan, alteren, inutilicen, supriman o dañen, la información, las bases de datos, los programas, los documentos electrónicos o cualquier clase de datos informáticos contenidos en cualquier soporte lógico, sistema informático, telemático, o en alguna de sus partes componentes .

4.2. ELEMENTOS DEL DELITO.

Los elementos que describen el tipo penal de daño en propiedad ajena son los siguientes:

- Sujeto (Activo y Pasivo).

- Conducta Típica.
- Medios de comisión.
- Resultado típico.
- Objetos material y jurídico.

Sujeto Activo.- Es quien realiza la conducta u omisión que produce el daño, deterioro o destrucción de la cosa ajena o propia en perjuicio de tercero. Puede ser cualquier persona. En el caso concreto del delito de daño en propiedad ajena vía Internet cometido en perjuicio de terceras personas que dependen de instituciones dedicadas a los estudios e investigación en las ciencias medicas, el Sujeto Activo será el hacker, cracker o cualquier otra persona, que cometa el ilícito.

Sujeto Pasivo.- Es sobre quien recae el daño patrimonial. En el caso concreto pueden ser Sujeto Pasivo las personas físicas o morales a quien el Sujeto Activo provoca el daño, estoy hablando de las instituciones dedicadas a la investigación y estudios de las ciencias médicas y a los terceros que de ellas dependen.

Conducta Típica: En la modalidad del delito que estudiamos seria destruir, alterar, inutilizar, suprimir o dañar, la información, las bases de datos, los programas, los documentos electrónicos o cualquier clase de datos informáticos contenidos en cualquier soporte lógico, sistema informático, telemático, o en alguna de sus partes componentes .

Medios de comisión: El tipo penal no exige ningún medio comisivo, por tanto solo agregaremos que puede tratarse de un medio comisivo (acción) u omisivo (omisión). Posteriormente mencionare brevemente cuales pueden ser los medios de comisión al caso concreto.

Resultado Típico.- Es cuando se destruye, altera, inutiliza, suprime o daña, la información, las bases de datos, los programas, los documentos electrónicos o cualquier clase de datos informáticos contenidos en cualquier soporte lógico, sistema informático, telemático, o en alguna de sus partes componentes, o bien simplemente se coloca en estado o situación de peligro al bien.

Objeto Material.- Es el daño producido en la cosa en si.

Objeto Jurídico.- Es el daño producido en el patrimonio.

4.3. SUJETO ACTIVO Y SUJETO PASIVO.

• 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.

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.

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.

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

William Spernow, otro criminólogo norteamericano, al considerar la diferencia entre un crimen tecnológico y uno de cuello blanco, destaca que en muchos casos son lo mismo. Si alguien por teléfono invita a otra invertir en una empresa fraudulenta, esto es un crimen de cuello blanco. En tanto, que un "delincuente técnico" podría mandar cientos de correos electrónicos con el mismo tema para vaciar las cuentas bancarias de sus víctimas.

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

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico

de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a si mismos "respetables" otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

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

Pero hablando de la modalidad de daño en propiedad ajena vía Internet en perjuicio de terceras personas, las cuales dependen de instituciones dedicadas a el estudio e investigación de las ciencias médicas, el Sujeto Activo es quien realiza la conducta u omisión que produce el daño, deterioro o destrucción de la cosa ajena o propia en perjuicio de instituciones dedicadas a los estudios e investigación en las ciencias médicas y de los terceros que dependen de esta.

• SUJETO PASIVO

En menester distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones dedicadas a la investigación y estudios de las ciencias médicas, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever

las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son 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 a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, 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.

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

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.

En el caso concreto pueden ser Sujeto Pasivo las personas físicas o morales a quien el Sujeto Activo provoca el daño, estoy hablando de las instituciones dedicadas a la investigación y estudios de las ciencias médicas y a los terceros que de ellas dependen.

4.4. MEDIOS DE COMISIÓN

Como apuntamos anteriormente, el tipo genérico de daño en propiedad ajena no exige algún medio comisivo en especial, por tanto puede ser cualquier medio.

A continuación se mencionaran algunos de los posibles Medios de Comisión de delito de Daño en propiedad ajena en la modalidad que hemos estudiado a lo largo de la investigación.

- Computadora (ordenador).- El Sujeto Activo utiliza la computadora para acceder a la información que el Sujeto Pasivo guarda en su computadora, crear virus, gusanos, bombas cronológicas o cualquier programa o archivo, con el fin de provocar daños en el hardware o software del sujeto pasivo.

- Software.- Por medio del software de programación el Sujeto activo puede provocar daños, ya que lo utiliza para crear archivos, programas, etc. Con el fin de afectar al sujeto pasivo.

- Línea Telefónica.- La línea telefónica conectada a un MODEM es utilizada para conectarse a un servidor y así poder acceder a Internet, de esta manera el sujeto activo puede cometer el ilícito ya que puede entrar a la información contenida en la computadora del sujeto pasivo o enviar

algún archivo con la intención de dañar el hardware y/o el software del sujeto pasivo.

- Servidor o Proveedor de Internet.- Servidor son aquellas empresas que prestan el servicio de conexión a Internet, como ya se menciono con anterioridad tanto sujeto activo como sujeto pasivo contratan los servicios de un servidor, de esta manera el sujeto pasivo puede cometer toda clase de delitos informáticos.

4.5. LEGISLACIÓN INTERNACIONAL PARA EL CONTROL DE DELITOS INFORMÁTICOS.

España es uno de los países en donde se ha dado mayor importancia a la regulación y control de los delitos informáticos, por lo que es conveniente mencionar las organizaciones y legislación en este país.

Al respecto se ha creado la Comisión de Libertades e Informática (CLI) es una plataforma independiente de carácter no gubernamental que inició sus trabajos en Noviembre de 1990 y celebró su Asamblea General Constituyente en Abril de 1991.

La CLI tiene como objetivo promover de forma permanente y estable en todo el país el desarrollo y la protección de los derechos individuales y colectivos, con especial referencia al derecho a la intimidad, frente al mal uso de las Tecnologías Informáticas y de las Comunicaciones, fomentando en la opinión pública la conciencia sobre la importancia de este tema para el progreso de una sociedad democrática crecientemente tecnificada.

La CLI está formada actualmente por las siguientes entidades:

- ALMD (Asociación Española de Marketing Directo)
- APDHE (Asociación Pro Derechos Humanos de España)
- ATI (Asociación de Técnicos de Informática)

- CC.OO. (Confederación Sindical de Comisiones Obreras)
- CECU (Confederación Estatal de Consumidores y Usuarios)
- FRAVM (Federación Regional de Asociaciones de Vecinos de Madrid)
- Jueces para la Democracia
- UCE (Unión de Consumidores de España)
- UGT (Unión General de Trabajadores)

En la actualidad existen las siguientes comisiones de ámbito territorial relacionadas con la CLI: Askatasunak eta Informatika (Euskadi), Comisión de Libertades e Informática de Aragón, Comissió de Llibertats i d'Informática de Catalunya, Comissió de Llibertats i d'Informática de Valencia (CLI VA). Está en fase de creación la Comisión de Andalucía.

Principios básicos

- Se ocupa de la promoción de los derechos individuales y colectivos en todas las esferas en que aquellos puedan resultar amenazados o vulnerados por el uso indebido de las Tecnologías de la Información.
- Impulsa todas las acciones e iniciativas necesarias para cumplir su objetivo, en el marco de la Constitución y de las normas internacionales y dentro del respeto a las competencias y funciones de los distintos Poderes y Organismos Públicos.
- Es una plataforma no gubernamental, sin personalidad jurídica propia, e independiente de todos los poderes públicos y privados.
- Está integrada por entidades colectivas de la sociedad civil que se comprometen a cumplir su objetivo y principios básicos, y se adecuan a

sus reglas de funcionamiento.

- Establece relaciones de cooperación con organismos de similares características existentes en otros países, en especial los europeos y los latinoamericanos.

- Está abierta a la colaboración con todas las entidades públicas y privadas cuyos fines sean coincidentes con el objetivo marcado.

- Respeta en todos los aspectos la autonomía de las organizaciones que la componen.

El Código Penal español tiene varios artículos íntimamente relacionados con el tema que estamos tratando.

Son los siguientes:

(Nota previa: El concepto de días-multa introducido por el artículo 50 indica que la cuota diaria tendrá un mínimo de doscientas pesetas y un máximo de cincuenta mil pesetas. A efecto de cómputo, los meses son de treinta días y los años de trescientos sesenta días.)

Artículo 197

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

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes

informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

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

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

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

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con

las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

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

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

Artículo 200

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

Artículo 201

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

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

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

Artículo 211 (Nota: Tanto de este artículo como del siguiente puden surgir dos incognitas. ¿Se pueden considerar que son de eficacia semejante Internet y los medios de comunicación tradicionales? ¿Son responsables los administradores de sistema o las empresas propietarias de los servidores?).

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

Artículo 212

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

Artículo 248

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

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

Artículo 255

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

1. Valiéndose de mecanismos instalados para realizar la defraudación.

2. Alterando maliciosamente las indicaciones o aparatos contadores.

3. Empleando cualesquiera otros medios clandestinos.

Artículo 256

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

Artículo 263

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

Artículo 264

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

1. Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2. Que se cause por cualquier medio infección o contagio de ganado.

3. Que se empleen sustancias venenosas o corrosivas.

4. Que afecten a bienes de dominio o uso público o comunal.

5. Que arruinen al perjudicado o se le coloque en grave situación económica.

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

Artículo 270

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

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

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400

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

Artículo 536

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

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

Otros países que disponen de una legislación adecuada para enfrentarse con el problema son los siguientes:

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda

Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

Espionaje de datos (202 a)

Estafa informática (263 a)

Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271. 273).

Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático (303 b). destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito (266b)

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial , en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de sus sustancia o función de alteraciones de su forma de aparición.

Venezuela

Ley Especial Contra los Delitos Informáticos

Título I

Disposiciones Generales

Artículo 1

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

Artículo 2.-

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

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

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

realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 3.

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

Artículo 4.

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

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

Artículo 5

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

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

Título II

De los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.

Artículo 6.-

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

Artículo 7.-

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

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

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

Artículo 8.-

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

Artículo 9.-

Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando

los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Artículo 10.-

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

Artículo 11.-

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

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

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

Artículo 12.-

Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que

utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

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

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

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13.-

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

Artículo 14.-

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

Artículo 15.-

Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.-

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

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

Artículo 17.-

Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario

autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

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

Artículo 18-

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

Artículo 19.-

Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III

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

Artículo 20.-

Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las

cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

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

Artículo 21.-

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

Artículo 22.-

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

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

Capítulo IV

De los delitos contra niños, niñas o adolescentes.

Artículo 23.-

Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.-

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

Capítulo V

De los delitos contra el orden económico.

Artículo 25.-

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

Artículo 26.-

Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo

que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III

Disposiciones comunes.

Artículo 27.-

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

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

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

Artículo 28.-

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

Artículo 29.-

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

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

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

3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

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

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

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

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987.

Esta ley contempla los siguientes delitos:

Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

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

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5).- En este artículo se

sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programase 18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Llama la atención que el Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un

acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistema informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Considero importante destacar la enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente

llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

4.6. LEGISLACIÓN EN MÉXICO PARA EL CONTROL DE DELITOS INFORMÁTICOS

En México los delitos informáticos actualmente no están contemplados de manera adecuada. Si bien es cierto uso de la computadora no es tan generalizado como en los países de primer mundo, no es menos cierto que es necesario un adecuado análisis y tratamiento por la vía del Derecho.

La utilización de tipos penales generales por vía de extensión a este tipo de acciones puede provocar enormes errores de apreciación y por tanto, de punitividad.

La legislación en nuestro país protege mas a los derechos de autor de posibles delitos informáticos, sin lugar a dudas es necesario proteger de forma mas eficaz otros derechos. Como mas adelante apuntaremos el Código Penal Federal, solo contempla el delito de acceso ilícito a sistemas y equipos de informática en el artículo 211 bis al 211 bis7. A continuación serán plasmados los artículos en referencia.

ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

ARTICULO 211 BIS 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta

días multa.

ARTICULO 211 BIS 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTICULO 211 BIS 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

ARTICULO 211 BIS 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTICULO 211 BIS 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 211 BIS 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

ARTICULO 211 BIS 7. Las penas previstas en este Capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Como fue posible observar en los artículos anteriores no se regulan todos los posibles delitos informáticos, además, considero que tampoco se protegen de forma adecuada los derechos de personas físicas ni morales.

LEY FEDERAL DEL DERECHO DE AUTOR Y CÓDIGO PENAL FEDERAL

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Sobre el particular, y por considerar de interés el contenido de la exposición

de motivos, cuando esta ley se presentó ante la Cámara de Diputados, se expusieron algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

De esta forma, cuando se puso en marcha la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos, lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito, se presentaba también una iniciativa de Decreto de Reforma al Código Penal Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor".

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

En este orden, como se mencionó anteriormente, esta Ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece

las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

En este sentido, considero importante detenernos en los artículos 102 y 231. El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

Apreciamos que aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424 Bis, fracción II del Código Penal Federal del que se infiere la sanción al uso de programas de virus.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un delito informático debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etcétera.

Por otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las

infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "usar. reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

La redacción de estas fracciones tratan de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Tal y como hemos sostenido, México no está excento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

En este entendido, considero que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Así mismo, consideramos que la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este articulo.

Por lo anterior, el análisis de este artículo corrobora la posición que hemos sostenido respecto a que en las conductas ilícitas relacionadas con la informáticas el bien jurídico a tutelar no es únicamente la propiedad intelectual sino todos aquellos derechos que se ponen en riesgo con los diversos delitos informáticos, por tal motivo este artículo no debería formar parte de una Ley de derechos de autor sino de una legislación especial tal y como se ha hecho en otros países.

Esta Ley, además establece en el Título X, en su capítulo único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultado para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal Federal.

De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión "fonogramas, videogramas o libros", además del verbo "reproducir", quedando:

"Art. 231...

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar

copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".

Con las reformas al Código Penal Federal se especifica que:

"Art. 424-Bis

/. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, videogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos".

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado, y que por tal razón fue necesaria una segunda modificación, en abril del año 2001 para incluir la acción de "reproducción".

De igual forma el artículo 424 que había sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril año pasado para incluir la reproducción y su comisión en una forma dolosa.

CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Consideramos que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

CONCLUSIONES

PRIMERA. En la actualidad el uso de la computadora a llegado a ser indispensable, al grado que en algunos casos se hacen operaciones muy importantes por medio de la computadora.

Actualmente las instituciones utilizan con más frecuencia las computadoras para manejar y almacenar su información, esto les trae muchos beneficios, pero también las hace un blanco al crimen por computadora (delitos informáticos). Las empresas están invirtiendo una parte de su presupuesto a la seguridad de sus sistemas.

SEGUNDA. Dentro de los delitos cometidos por computadoras, se pueden mencionar el robo, destrucción o modificación de información, fraude, entre otros y son realizados por personas con algún conocimiento de computación, ya sea dentro o fuera de la empresa.

Se considera que los delitos por computadora de mayor incidencia son el sabotaje informático (daño en propiedad ajena vía Internet) y la piratería de software, este ultimo se comete muchas veces sin saber que se está incurriendo en un delito y también sin tomar en cuenta la enorme perdida que esto significa para las empresas creadoras de software, es importante mencionar que este delito tiene una alta incidencia debido también a las cuestiones económicas en las que se vive. Con respecto a las legislaciones actuales, aún no se han abarcado todos los aspectos de este tipo de delitos, por lo que la mayoría de las veces son cometidos sin que haya una sanción adecuada. Sin embargo no se puede tener datos estadísticos confiables debido a la naturaleza de este delito.

TERCERA. Desafortunadamente en nuestro país, aún no se ha podido lograr una cultura dentro de las organizaciones con respecto a la protección de la información a través de la implantación de políticas, procedimientos y medidas de seguridad. La importancia de establecer dichas medidas proviene del gran valor

que la información representa para las empresas. Así mismo la falta de principios éticos en algunos profesionistas y usuarios de sistemas ha dado lugar a que este problema se agrave y se vuelve cada vez más común.

CUARTA. La seguridad informática debe promover la integridad, disponibilidad y confidencialidad de los sistemas, desde el punto de vista del hardware, software y datos, sin sacrificar su independencia y flexibilidad.

QUINTA. Hoy en día, existen varias técnicas y herramientas para proteger la información, entre ellas cabe mencionar la implantación de políticas de seguridad, uso de cortafuegos, claves de acceso, encriptado y codificado de mensajes, entre otros.

SEXTA. Se ha tenido un aumento crítico de crímenes por computadora, en atención a esto la agencia DISA (Agencia defensa de sistemas de información, www.disa.mil), del Pentágono, pidió a principios de 1996 a conocidos hackers que intentaran penetrar en su sistema informático: "el 88 por ciento de los ataques fueron exitosos, de este 88 por ciento el 96 por ciento no fueron detectados". John McConnell, director del NSA (Agencia Nacional de Seguridad, www.hpcc.gov/blue94/section.4.5.html), el más importante órgano norteamericano dedicado a la seguridad en su país, dijo durante un seminario: "Somos la nación más vulnerable de la Tierra".

El informe del Pentágono, "White paper on information infraestructure assurance" ("Documento blanco sobre la seguridad de la infraestructura de información"), lo confirma: "el sistema telefónico, los bancos, la Reserva Federal, la distribución de electricidad y combustible, el control del tráfico aéreo y otros sistemas inteligentes de transporte, la sanidad pública, las fuerzas de la ley e incluso el sistema de las elecciones dependen totalmente de las redes". Sólo en Estados Unidos, los daños por ataque vía Internet a las empresas, que casi nunca se denuncian, ascendieron en 1995 a 5,000 millones de dólares.

Según recientes estudios de, el 20% de las empresas norteamericanas que operan con redes abiertas de ordenadores sufrieron ataques piratas en 1993 y 1994. Las pérdidas económicas derivadas de las incursiones superaron los 250,000 dólares. Una cantidad sólo anecdótica, por que el 57 por ciento de las compañías se negó a dar cifras.

SÉPTIMA. Paradójicamente, y según los expertos, la principal arma de los hackers es la falta de previsión en seguridad de los usuarios de Internet, ya sean particulares o empresas.

OCTAVA. Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Hay un número no despreciable de personas poco honestas en las redes: fisgones que quieren curiosear morbosos que buscan violentar los sistemas; espías industriales y ladrones digitales. A todos estos se los ha englobado bajo la denominación de hackers, pero existen matizaciones. El término (que en castellano significa "CORTADOR") se suele aplicar a las intrusiones no dañinas, provocadas normalmente por simples fisgones que quieren probar que se puede violar un sistema de seguridad. Para las acciones nocivas existe la más contundente expresión CRACKER ("rompedor"). Las acciones de los crackers pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender, denominado "robo económico". Las familias de piratas navegan en barcos distintos. Incluso utilizan en los mensajes entre ellos "jergas" diferentes. Para referirse a la piratería, los norteamericanos distinguen entre "chicos buenos" y "chicos malos". Los chicos buenos buscan los agujeros de seguridad en los sistemas (una línea mal escrita entre las miles que forman los programas) y avisan del fallo a las empresas.

NOVENA. Los "criminales informáticos" accedieron en 1995, 162,500 veces a las bases del centro neurálgico de la "mayor potencia militar del planeta", los EE.UU.

DÉCIMA. Los últimos ataques cibernéticos a la fuerza aérea norteamericana (US Air Force) se han llevado a cabo por piratas rusos.

DÉCIMA PRIMERA. Jim Stile, exresponsable del FBI, dijo: "Denme 10 piratas y en 90 días este país se pondrá de rodillas".

DÉCIMA SEGUNDA. Según estimaciones del servicio Compuserve el 60% de las comunicaciones entre proveedores y distribuidores de estupefacientes se realizan a través de la Red.

DÉCIMA TERCERA. El Subcomité Permanente de Investigaciones del Senado norteamericano estimó el costo producido por ataques a sistemas informáticos de empresas, durante el año 1995, en 800 millones de dólares, sin contar las perdidas que muchos bancos no declaran por evitar la mala propaganda que ello supone.

DÉCIMA CUARTA . Algunos delincuentes usan computadoras, módems y otro equipo para robar bienes, dinero, información, software y servicios. Otros usan caballos de Troya, virus, gusanos, bombas lógicas y otros trucos de software para sabotear sistemas.

DÉCIMA QUINTA . Actualmente existen programas antivirus que están diseñados para buscar virus, identificarlos, notificar a los usuarios de su existencia y eliminarlos, de los discos o archivos infectados. Según los medios de comunicación, estas infracciones a la ley son cometidas por jóvenes y brillantes genios de la computación, los llamados hackers o crackers.

DÉCIMA SEXTA. Uno de los delitos por computadora más común como se menciono anteriormente es la piratería de software, es cometido por millones de personas, muchas veces sin saberlo. La piratería es una violación a las leyes de propiedad intelectual, las cuales muchas veces van a la zaga con respecto a la tecnología. Es hacer copias ilegales del programa que tiene Copyright (derechos de autor).

DÉCIMA SÉPTIMA . Otro delito muy común y el cual fue objeto de investigación en el presente trabajo es el sabotaje informático (daño en propiedad ajena), el cual como ya sabemos puede traer como consecuencia si hablamos de instituciones de dedicadas a los estudios e investigación de las ciencias medicas, problemas como el simple daño patrimonial hasta perdidas tan graves como pueden ser investigaciones sobre tratamiento y cura de enfermedades que en la actualidad cobran un sin numero de vidas.

DÉCIMA OCTAVA. Las medidas de seguridad se han creado para proteger nuestra intimidad y otros derechos individuales. Sin embargo, en ocasiones estos procedimientos de seguridad amenazan dichos derechos. Los estándares de seguridad y libertad de las computadoras generan importantes problemas de carácter jurídico legal y ético.

DÉCIMA NOVENA. Como nuestra sociedad emplea las computadoras en aplicaciones militares que ponen en juego la vida de la gente, los problemas de confiabilidad son muy importantes. En las aplicaciones militares modernas, la seguridad y la confiabilidad son aspectos críticos. Conforme vaya aumentando la velocidad, la potencia y la complejidad de los sistemas de armamento, muchos temen que los seres humanos sean excluidos del proceso de toma de decisiones. El debate sobre armamento de alta tecnología ha presentado por primera vez al publico problemas importantes de seguridad.

VIGÉSIMA. La preocupación por los delitos informáticos ha aumentado en los últimos años desde que cierta parte de la sociedad ha caído en cuenta del tremendo potencial que existe para la comisión de estos delitos en gran escala.

VIGÉSIMA PRIMERA. Los delitos de computadora y alta tecnología hacen que en ocasiones sea imposible pensar con los conceptos de derecho tradicionales y más aún el expresarse con el lenguaje tradicional; esto crea nuevas e inquietantes preguntas para los abogados a veces difíciles de responder, por tal motivo es necesario:

- Prevenir al publico en general sobre la realidad de este nuevo fenómeno delictivo y lograr que exija documentación sobre las medidas de seguridad que a nivel informático le ofrecen las entidades o personas que manejaran sus datos personales o sus bienes en forma computarizada.

- Alertar a los usuarios sobre la posibilidad de la ocurrencia de estos crímenes y delitos, animándolos a buscar y cerrar toda brecha de seguridad que exista en sus sistemas computarizados. Gran parte de los problemas se encuentra en la inacción de la víctima potencial; las organizaciones que dependen cada vez mas de las computadoras deben llegar a tener conciencia de que las medidas de seguridad mas que un gasto, son una inversión.

- Hacer una aportación seria a la doctrina jurídica para que tanto los abogados como otras personas interesadas tengan una fuente a donde acudir, para lo que sin lugar a dudas será una de las ramas del derecho mas litigadas en los próximos años, el derecho relacionado con las computadoras.

- Concientizar al legislador sobre la necesidad de la elaboración de leyes que incriminen y castiguen adecuadamente los llamados delitos informáticos y alta tecnología y otras infracciones relacionadas.

BIBLIOGRAFÍA

Aldegani, Gustavo. Seguridad informática. Argentina 1977. Edit. MP ediciones.

Ginzburg, Mario C. La PC por dentro. Argentina 1999. Edit. Publicación UAI.

Ginzburg, Mario C. Introducción General a la Informática. Argentina 1999. Edit. Publicación UAI.

González, de la Vega Francisco. Derecho penal mexicano. México 1990. Edit. Porrúa.

Hoffman, Paúl. Internet. México. 1995. Edit. Mc Graw-Hill.

Hoffman, Paúl. Internet manual de bolsillo. México 1995. Edit. Mc Graw-Hill.

Jiménez Huerta Mariano. Derecho penal mexicano IV. México 1984. Edit. Porrúa.

Klander, Lars. A prueba de Hackers. Argentina 1988. Edit. Anaya Multimedia.

Lima, de la Luz María. Delitos electrónicos. México 1984. Edit. Porrúa.

López, Betancurt Eduardo. Delitos en particular I. México 1994. Edit. Porrúa.

Laredo, Hill Adolfo. Derecho Autoral mexicano. México 1990.

Mora, José Luis. Introducción a la informática. México 1985. Edit. Trillas.

Paredes, Olea Héctor. Conceptos básicos de computación. México 1997. Edit. Trillas.

Seara, Vázquez Modesto. Derecho internacional público. México 1998. Edit. Porrúa.

Téllez, Valdes Julio. Derecho informático. México 1996. Edit. Mc Graw-Hill.

Ureña, López Alfonso. Fundamentos de informática. México 1999. Edit. Alfaomega.

LEGISLACIONES

Constitución Política de los Estados Unidos Mexicanos.

Código Penal Federal. México.

Ley Federal de Derecho de Autor.

Código Penal y de Procedimientos Penales de Sinaloa México.

Código penal Español.

Acta Federal de Abuso Computacional. E.E.U.U. 1994.

Ley contra la Criminalidad Económica. Alemania.

Ley de Delitos Informáticos. Venezuela.

Ley de Reforma del Código Penal del 22 de diciembre de 1987. Austria.

Ley número 88-19 de 5 de enero de 1988. Francia.