UNIVERSIDAD LA SALLE

FACULTAD DE DERECHO

INCORPORADA A LA U.N.A.M.

"LOS DELITOS COMETIDOS POR MEDIO DE INTERNET"

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN DERECHO

PRESENTA

VICTOR MANUEL HERRERA CABRERA

ASESOR DE TESIS

LIC. RICARDO AUGUSTO HERRERA TENORIO

MEXICO, D.F. **2009**

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ANEXO 13

AUTORIZACIÓN DE IMPRESIÓN DE TESIS

C. DIRECTOR GENERAL DE INCORPORACIÓN Y REVALIDACIÓN DE ESTUDIOS
U N A M
PRESENTE

Me permito informar a usted que la tesis titulada: "Los Delitos cometidos por medio de Internet"

Elaborada por:

Herrera	Cabrera	Víctor Manuel
Apellido Paterno	Apellido Materno	Nombre (s)

Alumno(a) de la carrera de la Licenciatura en Derecho

No. de Cta. 837040149

reúne los requisitos académicos para su impresión.

16 de Octubre 2008.

Lic. Ricardo Augusto Herrera Tenorio		Mtro. Jorge Nader Kuri
Nombre y firma del Asesor de Tesis	Sello de la Institución	Nombre y firma del Director de la Escuela ó Facultad

A mis padres, que con su ejemplo me han permitido
Cumplir con este sueño, hoy hecho realidad.
Mamá, Papá. Muchas Gracias.

A mi esposa por impulsarme cada día
En la conclusión de este trabajo.
Gracias Miriam.

C A P I T U L A D O

“LOS DELITOS COMETIDOS POR MEDIO DE INTERNET”

INTRODUCCIÓN Pág. 4

CAPÍTULO PRIMERO “ANTECEDENTES HISTÓRICOS DE LA COMPUTACIÓN” Pág. 8

I.- LA COMPUTADORA Pág. 8

II.- SU FUNCIÓN Pág. 18

III.- EL INTERNET Pág. 32

IV.- QUE ES EL CIBERESPACIO Pág. 41

V.- LA TRANSFERENCIA DE CRÉDITO A TRAVÉS DEL INTERNET O TRANSFERENCIA ELECTRÓNICA Pág. 42

VI.- SU USO EN LA ACTUALIDAD Pág. 52

CAPÍTULO SEGUNDO "LOS DELITOS QUE SE COMETEN POR MEDIO DE INTERNET" Pág. 57

I.- EL CRIMEN COMPUTACIONAL Pág. 57

II.- EL ROBO DE PROGRAMAS Pág. 58

III.- VIRUS COMPUTACIONAL Pág. 67

IV.- ROBO DE LOS COMPONENTES FISICOS DE LA COMPUADORA O HARD WARE Pág. 71

V.- ROBO DE INFORMACION Pág. 73

VI.- DELINCUENTE CIBERNETICO O HACKER CRIMINAL . Pág. 76

VII.- COMPRAVENTA DE BIENES SIMULADOS Pág. 83

VIII.- TRANSFERENCIAS BANCARIAS DELICTUOSAS, FICTICIAS Y REALES Pág. 85

CAPÍTULO TERCERO "LOS DELITOS POR INTERNET" . Pág. 94

I.- CONCEPTO DEL DELITO Pág. 94

II.- CONCEPTO JURIDICO DEL DELITO Pág. 97

III.- EL HECHO Y SUS ELEMENTOS, LA CONDUCTA Pág. 100

IV.- TIPICIDAD Pág. 103

V.- ANTIJURICIDAD Pág. 106

VI.- CULPABILIDAD Pág. 108

VII.- PUNIBILIDAD Pág. 120

CAPÍTULO CUARTO "PROPUESTAS RESPECTO A LOS DELITOS COMETIDOS POR INTERNET" Pág. 122

I.- CONCEPTO DE DELITO INFORMATICO Pág. 122

II.- CARACCTERISTICAS DEL SUJETO ACTIVO Pág. 128

III.- CARACTERISTICAS DEL SUJETO PASIVO Pág. 132

IV.- CONCLUSIONES Pág. 138

BIBLIOGRAFÍA Pág. 153

INTRODUCCION

En el presente trabajo se pretende dar un panorama de la problemática que desde el surgimiento del Internet ha venido afectando a la sociedad por la comisión de diversos delitos que, conforme la tecnología evoluciona, estos se van sofisticando, llegando a ser muy difícil de que, en las agencias del ministerio publico y los juzgadores sobre todo, puedan aplicar sanciones por carecer actualmente nuestras leyes de la tificación de estos delitos.

Hoy día resulta por demás frustrante que los delincuentes salgan libres o en el pero de los casos que no se les pueda consignar por que no existe un tipo adecuado para estos ilícitos. Cabe mencionar que si bien es cierto que existen algunos Códigos Penales estatales que han comenzado a tipificar estos delito, incluso el Código Penal Federal, estos resultan insuficientes en atención a que no se profundiza en los medios que se emplean para la comisión de dichos ilícitos, es decir, nuestros legisladores deberían de ser mejor asesorados por expertos en el uso de las computadoras, Internet y medios electrónicos, para que

comprenda su funcionamiento y por consiguiente se puedan elaborar las normas que puedan ser aplicadas con toda claridad en la impartición de justicia.

Claramente el problema al que se enfrentan los juzgadores pero sobre todo los legisladores en la impartición, pero en especial en la creación de las normas con las que se pueda sancionar los delitos que se cometan por medio del Internet o medios electrónicos, es que, no se conocen a fondo el funcionamiento de los medios empleados por los delincuentes para la comisión de esos delitos, que van desde la computadora, programas o software e Internet, hasta la esfera de competencia de los juzgados que conocerán de los juicios, cuando esto debería quedar en la competencia federal por los medios que en su mayoría son empleados.

Como ejemplo podemos señalar el hecho de que un individuo usando el Internet y algún programa desde su computadora en Villahermosa, pueda ingresar a la computadora de una persona que vive en Guadalajara para que cuando utilice su contraseña para efectuar alguna

transferencia electrónica con su banco, el primer sujeto copie dicha contraseña y posteriormente la utilice en su beneficio y sin la autorización del titular de la cuenta bancaria. Siendo este el típico caso de competencia que autoridad seria la que conocería del caso, Villahermosa en donde se encontraba el sujeto que cometió el ilícito o bien Guadalajara que es donde se encuentra el sujeto pasivo o victima del ilícito.

Pues bien, con este ejemplo considero pertinente que quien debe conocer de este tipo de ilícitos sea el fuero federal, ya que se utilizan medios de comunicación mismos que están reglados por legislación federal y por consiguiente debe conocer de estos casos la Procuraduría General de la Republica y los Juzgados de Distrito en materia penal.

Por lo anterior en el presente trabajo en lo que mas se ahonda es el aspecto del conocimiento de la computadora e Internet, para posteriormente hacer un análisis sencillo de los elementos del delito en forma general y finalmente la sugerencia de lo que al criterio de un servidor se deben considerar como los elementos de los delitos

cometidos por medio del Internet y una propuesta de lo que considero sea la clasificaron de estos delitos.

Es cierto que en el presente trabajo hago mucha referencia a aspectos técnicos pero de verdad que es muy importante conocer de estos antecedentes para poder entender la comisión de los delitos, ya que quienes nos hemos enfrentado a las lagunas que presenta nuestra legislación penal con frustración y tristeza vemos que por no estar preparados desde los agentes del ministerio publico hasta nuestros legisladores, se continúan dejando en libertad a aquellos que usando estos medios para cometer sus ilícitos no son castigados por no existir las normas adecuadas para que sean sancionados. Y lo que es peor, que continúen cometiendo estos ilícitos en detrimento de los individuos en particular y de la sociedad en general.

CAPÍTULO PRIMERO “ANTECEDENTES HISTÓRICOS DE LA COMPUTACIÓN”

I.- LA COMPUTADORA

La computadora el instrumento más útil de nuestros días, ha venido revolucionándose así misma con una gran velocidad, es así que las computadoras de los años 60, las cuales ocupaban grandes espacios, hoy en día son tan pequeñas que se les puede transportar en viajes de negocios, de esta forma, para hablar de la computadora se tiene que realizar un pequeño repaso por sus antecedentes históricos.

Tanto en la antigüedad como en la época contemporánea las civilizaciones siempre han buscado facilitarse el trabajo, para lograr tal objetivo se ha recurrido a la ciencia, es el caso que en la civilización maya, a partir del cero lograron definir el ciclo lunar con un error inferior a ocho horas en trescientos años. Esta civilización no sólo inventó el concepto de cero, hecho que según los expertos fue el precedente a lo que equivalió al de los hindúes, sino que los mayas

fueron los que desarrollaron un calendario a base de agudas observaciones científicas y cálculos muy precisos; este calendario puede ser proyectado cronológicamente con una validez extraordinaria hasta por un lapso de trescientos mil años.

Los grandes avances de la ciencia y la tecnología se han dado en función del tiempo, es decir, se han ido logrando los avances de acuerdo a las grandes necesidades que ha requerido la humanidad, de ahí la sensación de brincar de la prehistoria a nuestros días de manera muy dramática. En cuanto al desarrollo de la computadora, ésta ha tenido una evolución tremenda, ya que nadie hubiera imaginado que hoy en día en casi cualquier hogar se pueda contar con una, (al menos en los países desarrollados y espero que en un futuro no muy lejano también lo podamos observar en los países en vías de desarrollo como México), que en sus comienzos, fuera muy lenta por funcionar con palancas y ruedas, pasando por el inicio del procesamiento de datos hasta llegar a los micro chips y la fibra óptica.

Aproximadamente a partir del año de 1951, a computadora ya se había introducido al mercado en forma comercial, pero ni siquiera aquellos que estaban en contacto con ella, estaban preparados para ver lo que vendría después, ya que el desarrollo tan acelerado que ha presentado la computadora en términos de capacidad, tamaño y potencia, así como de costo de operación, ha constituido una de las grandes sorpresas de nuestros días. Lo que tal vez no sea tan sorprendente, es que el éxito alcanzado por la computadora se debe en gran medida al esfuerzo de muchas personas por resolver los problemas en los diferentes campos, dando por consecuencia que el desempeño de nuestras actividades sea aun más fácil con el apoyo de la computadora.

Es por eso que el éxito que ha alcanzado la computadora se debe en gran medida a la enorme capacidad de almacenar y procesar cantidades muy grandes de información. La computadora puede agregar más datos a la información ya existente, la actualiza y transmite a lugares muy lejanos a través del uso de satélites o líneas telefónicas. Así mismo, la computadora puede efectuar cálculos, establecer comparaciones, simular hechos y controlar operaciones

científicas e industriales con hechos reales, es decir, que están ocurriendo en realidad.

Todas estas funciones provienen de la facultad básica de la computadora que consiste en procesar y almacenar datos en forma de códigos numéricos. La computadora ha tenido una evolución a partir de los primeros instrumentos o inventos utilizados para contar, como por ejemplo el ábaco, hoy en día se han dejado a un lado las cuentas de los antiguos aparatos para sustituirlos por los impulsos electrónicos para no solamente alcanzar los mismos objetivos, si no para superarlos en mucho.

Una de las cosas que ha beneficiado a las computadoras en su proceso de evolución, es que gracias a la gran competencia de los fabricantes de esos instrumentos, el costo de las computadoras ha descendido considerablemente y por esa razón, éstas ya no se encuentran únicamente destinadas para usos científicos, militares o gubernamentales, sino que ahora cualquier persona puede adquirir un equipo de cómputo sin ninguna restricción. En la época contemporánea, es factible encontrar que la computadora puede

realizar aplicaciones que hasta hace unos años se consideraban impracticables.

La gran celeridad con que la computadora ha evolucionado, ha dado origen a que los implementos con los que se construyen las computadoras, se sustituyan con una gran rapidez, como ejemplo de este continuo crecimiento y mejoramiento de los componentes tenemos que los contadores electromecánicos fueron transformados por los bulbos; el almacenamiento y memoria magnética, dio origen a que surgieran los circuitos microscópicos de estado sólido y así sucesivamente un implemento ha dado origen a otro pero mejorado.

En realidad la computadora es una máquina asombrosa y pocas herramientas de trabajo pueden permitir el que se realicen tantas tareas y todas diferentes entre sí, ya sea que se quiera dar seguimiento a una inversión, publicar un periódico, diseñar un edificio, realizar simulaciones científicas con un grado de error muy bajo, entre otros muchos usos que puede apoyar con la computadora.

Actualmente las computadoras de uso general presentan muchos tamaños y capacidades. Los términos que describen en la actualidad a las computadoras por su tamaño son los siguientes: Súper-computadora, Macro-computadora, Mini- computadora, Estación de trabajo y Computadora personal. Todos y cada uno de estos tipos de computadoras pueden conectarse entre sí para formar redes de computadoras.

SUPER-COMPUTADORA

La súper-computadora es la computadora más potente disponible en un momento dado. Estas máquinas están construidas para procesar enormes cantidades de información en forma muy rápida, por ejemplo, este tipo de computadoras son utilizadas por los científicos para ejecutar pruebas de fisión nuclear, sin que se corran los riesgos de una explosión accidental o una explosión nuclear que ponga en grave riesgo vidas inocentes de la población.

De los inconvenientes que presentan este tipo de súper-computadoras es que generan una gran cantidad de calor por su tamaño, el elevado consumo de energía y desde luego, su costo que es muy elevado.

MACRO-COMPUTADORA

Las computadoras de mayor tamaño de uso común son las macro-computadoras, éstas están diseñadas para manejar grandes cantidades de información tanto de entrada, salida y almacenamiento. Un ejemplo de éstas es la computadora central de un grupo de tiendas departamentales, en donde por cada tienda existen varias terminales que son utilizadas por los empleados.

La terminal es una especie de computadora que no tiene CPU propio, es solamente un dispositivo de entrada y salida que actúa como una ventana hacia otra computadora central que se encuentra en alguna otra parte fuera de la tienda.

CPU cuyo significado es unidad de procesamiento central, término que se utiliza exclusivamente para referirse al procesador de una computadora, ya sea una serie de tarjetas de circuitos o sólo micro-procesador. En el CPU, se encuentra la inteligencia de la computadora y es donde se realizan los cálculos y decisiones.

MINI-COMPUTADORA

Cabe destacar que en un inicio solamente existían computadoras en términos generales y no había clasificación al respecto, pero a partir de que empezaron a salir nuevos tipos de computadoras, surgió la necesidad de implementar otros términos para poder distinguir los diferentes tipos. La primera empresa en utilizar el nombre de mini-computadoras, fue la DEC (Digital Equipment Corporation) quien comercializó en los años sesenta un tipo de computadora más pequeña que las que en ese entonces se utilizaban, denominándola mini-computadora. Más tarde, cuando surgieron computadoras más pequeñas en las que se instalaban micro-procesadores, se les llamó micro-computadoras y eventualmente computadoras personales.

ESTACIONES DE TRABAJO

Entre las mini-computadoras y las micro-computadoras existe una clase de computadoras conocidas como estaciones de trabajo. Estas se ven como computadoras de tipo personal o computadoras personales, ya que son utilizadas por una sola persona, al igual que una computadora personal, aunque en el caso de las estaciones de trabajo, éstas presentan una mayor capacidad que las computadoras personales. Además de la capacidad, otra diferencia entre la estación de trabajo y las computadoras personales, es que estas últimas, pueden correr cualquiera de los sistemas operativos que se encuentran en el mercado, a diferencia de las estaciones de trabajo que únicamente pueden correr el sistema operativo Unix o la variación de este.

COMPUTADORAS PERSONALES

Cuando las personas utilizan el término computadoras personales o micro- computadoras, generalmente lo hacen para referirse a las

computadoras que se encuentran en las oficinas, escuelas y casas. Estas computadoras vienen en varios modelos y tamaños, éstas por lo general, son colocadas en los escritorios de las oficinas, aunque también las colocan en el piso y hasta las hay tan pequeñas que son portátiles. Los términos mini-computadora y computadora personal, son intercambiables aunque también se les denomina PC (del inglés, Personal Computer). Esta denominación fue utilizada por vez primera por la empresa IBM, para la primera micro-computadora que fabricó.

El primer modelo de computadora personal fue el modelo de escritorio, el cual es hasta hoy, el modelo más conocido por todas las personas y más vendido, ya que por su tamaño fácilmente puede caber en un escritorio, y a pesar de que son pequeñas, no lo son tanto como para llevarlas de viaje.

También están consideras como computadoras personales las llamadas notebook (cuya traducción al español es libro de notas) o portátiles, que como su nombre lo indica son del tamaño de un cuaderno o carpeta tamaño oficio y son las predecesoras a las Lap Top; aunque un

poco más grandes, cuentan con todas las características de una computadora personal, en cuanto a capacidad, teclado y pantalla.

II.- SU FUNCIÓN

Son varias las formas en que se utilizan las computadoras y nos muestran lo poderosas que son por su capacidad de almacenar información, pero ¿Cómo funcionan?; independiente del tamaño o forma de las computadoras, estas están compuestas de cinco elementos que son:

1.- Un procesador.

2.- Memoria.

3.- Dispositivos de entrada y salida.

4.- Discos de almacenamiento.

5.- Programas.

Los primeros cuatro elementos que integran o componen a la computadora también son denominados como “hardware”, que no es

otra cosa que los elementos físicos y tangibles de que esta compuesta una computadora.

El quinto componente de una computadora es denominado “software”, y no es otra cosa que las instrucciones electrónicas para que el hardware ejecute lo que una persona quiere realizar a través de la computadora.

1.- El Procesador.- no es sino un complejo procedimiento que transforma los datos nuevos de entrada y salida al que se le llama procesamiento. El procesador hace las funciones de cerebro de la computadora que interpreta y ejecuta las instrucciones. Para el caso de las computadoras grandes, el procesador está compuesto de varios chips o circuitos integrados, mismos que están fabricados en rebanadas de silicio u otro material en donde se encuentran grabados los circuitos electrónicos diminutos. Estos chips están insertados en tarjetas de circuitos electrónicos diminutos. En las computadoras personales el procesador es un solo chip llamado micro-procesador.

2.- Memoria.- La CPU utiliza la memoria de la computadora para guardar piezas de información mientras trabaja con ellas y como un tablero de recortes para realizar los cálculos. Esta información es representada electrónicamente en los circuitos de los chips de la memoria y, mientras permanezca en la memoria, la computadora puede tener acceso directo a dicha información. Esta memoria constituida internamente se llama memoria de acceso aleatorio también conocida como RAM. Entre más RAM tenga una computadora, más cosas puede hacer, ya que la cantidad de memoria de una computadora afecta sus capacidades. La unidad más común para medir la memoria de una computadora es el byte. El byte se puede definir como la cantidad mínima de memoria que se necesita para guardar un solo carácter.

3.- Dispositivos de entrada y salida.- La entrada y salida o E/S, I/O por sus siglas en inglés, comprenden todas las maneras en que una computadora se comunica con el usuario y con otras máquinas o dispositivos. Los dispositivos de entrada aceptan datos e instrucciones del usuario. Los dispositivos de salida regresan datos procesados, esto

es, información al usuario. Sin estos dispositivos de entrada y salida, la computadora se encontraría aislada. No podría recibir instrucciones y si las tuviera grabadas en forma permanente, no podría comunicar los resultados de su trabajo.

Ejemplos de dispositivos de entrada son el teclado, mouse o ratón, las palancas de juegos o joysticks y los rastreadores o scanners.

La función de los dispositivos de salida es presentar datos procesados (información) al usuario. Los dispositivos de salida más comunes son la pantalla o monitor y la impresora. La computadora envía la información de salida al monitor cuando el usuario necesita únicamente ver la información. Cuando el usuario necesita una copia física de la información, la computadora envía esta información a la impresora, los sistemas multimedia, pueden incluir las bocinas como dispositivos de salida.

4.- Almacenamiento.- La computadora puede funcionar nada más con el procesador, la memoria y los dispositivos de entrada y salida. Sin embargo, para ser realmente útil, necesita un lugar donde guardar los datos que no está procesando en ese momento. El propósito del almacenamiento es guardar datos que la computadora no esté usando.

Es útil pensar en el almacenamiento como si fuera un archivero electrónico y en la memoria como si fuera una mesa de trabajo electrónica. Cuando se necesite trabajar con esa serie de información, la computadora la extrae del archivero y la pone sobre la mesa de trabajo, y cuando ya no la necesita, la computadora regresa de nueva cuenta la información al archivero. Aunque el procesador no puede trabajar directamente con los datos del archivero, el almacenamiento tiene tres ventajas sobre la memoria. Primero, hay más espacio de almacenamiento que en la memoria; segundo, el almacenamiento retiene el contenido de la información cuando se apaga la computadora y; tercero, el almacenamiento es mucho más barato que la de la memoria.

El medio de almacenamiento más común es el disco magnético o disquete, como su nombre lo indica, el disco es un objeto redondo y plano que gira alrededor de su centro. Las cabezas de lectura y escritura, son similares a las cabezas de una grabadora o una video-reproductora, las cuales flotan por encima o por debajo de la superficie del disco.

El dispositivo que contiene al disco se llama unidad de disco o “drive”, algunos discos están integrados a su unidad y no se pueden remover. Existe otro tipo de unidades que se pueden remover y ser reemplazados. La mayoría de las computadoras personales tienen un disco duro no removible, además usualmente hay una o dos unidades de disco flexible, las cuales le permiten usar discos flexibles removibles. Un disco duro, normalmente puede guardar muchos más datos que un disco flexible y por eso se usa el disco duro como el archivero principal de la computadora. Los discos flexibles se usan para cargar datos o programas nuevos al disco duro, intercambiar datos con otros usuarios o hacer una segunda copia de respaldo de los datos que están en el disco duro.

5.- Programa o Software.- En su mayor parte las computadoras son máquinas de uso general: muchas pueden ser usadas con la misma eficiencia para trabajar con números que para crear documentos o dibujos, o para controlar a otras máquinas. El componente que hace que una computadora realice una tarea específica es el programa o software, es decir, las instrucciones electrónicas que generalmente residen en un dispositivo de almacenamiento.

A un grupo específico de estas instrucciones se le llama programa. Cuando una computadora está usando un programa en particular, se dice que está corriendo o ejecutando ese programa. Debido a que los programas son los que dan las instrucciones que los componentes físicos de la computadora deben efectuar, sin los programas la computadora sería inútil y no podría hacer nada, sería prácticamente un adorno de metal y plástico.

Aunque la variedad de programas disponibles es vasta y variada, la mayoría del software puede ser dividido en dos grandes categorías: **i)** software operativo o de sistema y **ii)** software de aplicación.

Software operativo o sistema.- El software operativo es el principal ya que es el que indica a la computadora cómo usar sus propios componentes. Cuando se enciende la computadora, ésta ejecuta varios pasos preparativos para ser usada. El primer paso es realizar una auto-prueba, es decir, la computadora revisa cuales son los programas o dispositivos que se encuentran conectados a ella, cuenta la capacidad de memoria y por último, hace una rápida revisión para determinar si la memoria está trabajando en forma correcta.

Después que la computadora encuentra y arranca el sistema operativo está lista para aceptar dispositivos de entrada como el teclado y el mouse. Llegando a este punto, el usuario puede dar comandos a la computadora, como por ejemplo, hacer una lista de programas en el disco de la computadora o hacer que la computadora corra uno de esos programas.

Software de aplicación.- Una computadora que solamente corre o usa un sistema operativo, tampoco es de mucha ayuda, puesto que el sistema operativo es para el beneficio de la computadora, se requieren otros programas para hacer de la computadora algo útil para los usuarios.

Este término de software de aplicación, describe programas que son para el usuario, el cual ha sido diseñado para ser aplicado en determinada área así tenemos que existen software o aplicaciones para:

(i)Software para negocios

(ii)Software de utilerías

(iii)Software personales

(iv)Software de entretenimiento

(v)Software educativos

(i)Software para negocios.- Aún y cuando existe una tendencia creciente por el uso de la computadora en los hogares, la gran mayoría de las computadoras son utilizadas en ambientes comerciales de

negocios o industrialmente. Las aplicaciones más comunes e importantes son: **a)** los procesadores de palabras, **b)** las hojas de cálculo y **c)** las bases de datos.

a) Los procesadores de palabras son la versión moderna de las máquinas de escribir, con la gran ventaja de que se puede editar, revisar la ortografía y la gramática del documento e inclusive es posible cambiar el tipo de la letra.

El procesador de palabras se puede utilizar para la creación de cualquier tipo de documento entre otros: cartas de negocios, boletines, reportes informativos y hasta libros, sólo por mencionar algunos de sus usos.

b) Las hojas de cálculo, son procesadores de números. La primer versión de la hoy popular hoja de cálculo, fue aquella denominada VisiCalc y que fue desarrolladas para la computadora Apple II. El nombre VisiCalc es la abreviatura del nombre “Visible calculator” que en español se traduce como “calculadora visible”.

La hoja de cálculo, es un programa que despliega una matriz muy grande de columnas y renglones, de la que únicamente se puede observar una parte a la vez; al área donde se cruzan columnas y renglones, se le denomina celda.

En la hoja de cálculo se pueden poner textos, números, fórmulas, obteniendo de esta forma, una hoja contable computarizada. También se pueden generar gráficas y tablas para mostrar de una forma gráfica las relaciones entre los números.

Como la mayoría de los elementos de las computadoras, las hojas de cálculo han sufrido muchos cambios desde que fueron desarrolladas por primera vez. Actualmente una buena parte de las hojas de cálculo son tridimensionales permitiendo al usuario crear no sólo una hoja de cálculo, sino un legajo de hojas de cálculo con apariencia contable y que puede ligarse con otras vías electrónicas.

c) Las bases de datos dan la posibilidad de ampliar la información almacenada en la computadora del usuario y permite diversas formas

para la búsqueda de datos o información. La base de datos hace las veces de un archivero en donde generalmente la información o documentos se clasifica en una forma lógica, por lo común es en orden alfabético, dependiendo del nombre del documento a archivar.

Un ejemplo de una base de datos puede ser el hecho que en una tienda de autoservicio, se lleve un inventario de los productos que se venden, entonces si el usuario necesita un reporte de cual es la existencia de un producto determinado, se podrá tener el número de unidades existentes en el almacén.

(ii) Software de utilerías.- éstas representan la segunda categoría de aplicaciones con las que el usuario de la computadora, puede con ayuda de las utilerías, administrar y dar mantenimiento a la computadora que está usando.

Los programas de utilerías, ofrecen al usuario menús que permiten escoger con facilidad programas para correr dentro de los que destacan el utilizado para recuperar documentos borrados por

accidente o equivocación, incrementar la velocidad y eficiencia de la máquina y organizar la información en su sistema. Una muestra de este tipo de software es el llamado Norton Utilities, que no es otra cosa que un programa que proporciona al usuario una serie de herramientas y programas de mantenimiento para computadoras personales (PC's).

(iii) Softwares personales.- el avance tecnológico en el campo de las computadoras, ha propiciado que los creadores de programas o software, en forma constante saquen programas diseñados para quitar el tedio de las tareas personales y volverlas más divertidas y dinámicas.

Esta clase de programas permiten por ejemplo, mantener una agenda y calendario de citas, hacer las operaciones bancarias sin tener la necesidad de salir ya sea del trabajo o casa, enviar un correo electrónico, así como conectarse a bases de datos con información de utilidad para el usuario.

(iv) Software de entretenimiento.- en esta categoría de programas o software de entretenimiento entran los video-juegos, simuladores de vuelo, juegos de mesa tales como ajedrez, rompecabezas de difícil solución, entre muchos otros.

(v) Software educativos.- estos programas también pueden considerarse como de entretenimiento, como lo son aquellos programas que enseñan a los niños a multiplicar, reconocer el alfabeto, etc., ya que siempre son presentados con el formato de juegos, de tal suerte que los niños al jugar aprenden.

Pero, también existen programas educativos para adultos en los que no precisamente son juegos sino todo lo contrario, son programas serios en los que se encuentran enciclopedias, programas de Geografía, inclusive cursos de idiomas.

III.- EL INTERNET

¿Qué es Internet?

Concepto

Es un conjunto de computadoras conectadas entre sí situadas alrededor del mundo (más de 30'000,000 de computadoras). La información contenida en cada una de estas computadoras es accesible desde cualquier otra computadora conectada a esta red. No existe ninguna compañía que se llame Internet. No existe ninguna organización que imponga reglas. Aquellas organizaciones que quieren conectar sus computadoras a Internet no tienen más que enlazarse a otra computadora que, a su vez, esté en Internet. Cada organización es responsable de sus propias computadoras y de sus conexiones. Su mandato acaba donde terminan sus propios cables.

Historia

Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado ARPANET (Advanced Research Project Network), iniciado en 1969 y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para enlazar redes de transmisión de paquetes informáticos de diferentes tipos capaces de resistir las condiciones de operación más difíciles y continuar funcionando aún con la pérdida de una parte de la red (por ejemplo en caso de guerra).

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet. Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la red de redes más grande del mundo. Las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo

requiriese, sin importar de que país provenía la solicitud, siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión).

Los usuarios pronto encontraron que la información que había en la red era por demás útil y si cada quién aportaba algo se enriquecería aún más el acervo de información existente.

Por extraño que parezca, no existe una autoridad central que controle el funcionamiento de la red; aunque existen grupos y organizaciones que se dedican a organizar de alguna forma el tráfico en ella. Después de que las funciones militares de la red se separaron en una red secundaria de Internet, la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos la National Science Foundation la cual promovió bastante el uso de la red, ya que se encargó de conectar cinco centros de súper-cómputo a los que se podía acceder desde cualquier nodo de la red.

Esto funcionó bien al principio, pero pronto fueron superadas las cargas de tráfico previstas, entonces se dio la concesión a Merit Network Inc., para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando un servicio mucho más rápido, pero este proceso de mejora nunca termina, debido a la creciente demanda de los servicios que se encuentran en la red. El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada país que forma parte de Internet lo que proporciona un servicio prácticamente gratuito.

A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

Componentes del sistema

Más allá de las metáforas, Internet es:

En Internet, tu computadora puede comunicarse con cualquier otra computadora localizada en cualquier lugar del mundo. Internet es la

red de computadoras más grande del mundo operada por entidades públicas y privadas.

Las proyecciones indican que en un futuro cercano se alcanzará la cifra de 100 millones de usuarios. Nadie es dueño de Internet. No hay una computadora central de Internet. Por el contrario, Internet es el mejor ejemplo de la tecnología abierta.

Cualquier computadora puede comunicarse con otra, independientemente del tipo de sistema o de los programas utilizados. En algunos casos pueden ser necesarias ciertas interfaces para poder visualizar, escuchar o ver presentaciones multimedia. Éstas se pueden conseguir en Internet bajo el nombre de Plug-ins (enchufables).

Internet es una plataforma para la relación cliente/servidor. Un cliente es una aplicación de software, usualmente ejecutada en una PC o en una estación de trabajo UNIX, que le permite acceder, ver y trabajar con datos provistos por un servidor. Un servidor es una computadora y su software, que administra la información para los clientes. Todas

estas computadoras interconectadas entre sí pueden entenderse dado que utilizan un protocolo, es decir, una serie de reglas y convenciones.

Dos protocolos son esenciales para todas las comunicaciones a través de Internet: el Transmission Control Protocol y el Internet Protocol (protocolo de control de transmisión y protocolo Internet), conocidos comúnmente como TCP/IP. Otros protocolos gobiernan las actividades de Internet:

Correo Electrónico (E-Mail)

Usenet Newsgroups (grupos de interés)

File Transfer Protocol (FTP)

Telnet

HTTP/World Wide Web

El Correo Electrónico es un medio muy útil para comunicarse con los demás, ya sea que se encuentren en la misma oficina, en otro edificio, en otra ciudad o en otro país en el mundo.

Los Newsgroups, son grupos de usuarios a los que uno se puede suscribir para intercambiar opiniones o recibir información sobre temas actuales.

El FTP es el protocolo que permite enviar o recibir archivos en lugar de utilizar disquetes, por ejemplo. Estas transferencias pueden ser privadas o anónimas, es decir accesibles para todos aquellos que estén interesados.

El protocolo TelNet permite que nos podamos conectar a otro equipo como una estación de trabajo que no se encuentra en el mismo lugar físico. De esta manera podemos acceder a bases de datos y programas.

La World Wide Web o Telaraña Mundial, utiliza una nueva tecnología que te permite acceder a los recursos de Internet de una manera sencilla en un ambiente gráfico interactivo donde la información es fácil de encontrar y de acceder.

Lo que ha sido revolucionario en la WEB es el hipertexto. Los hipertextos relacionan información (enlaces) en un documento con información relacionada por medio de códigos de dirección. Un usuario sencillamente hace clic en un texto resaltado para alcanzar mayor detalle sobre un tema o saltar a un tema relacionado. Las claves de cómo funciona la WEB es el protocolo HyperText Transfer Protocol (HTTP) y el Hypertext Markup Language (HTML).

Poniéndolo de manera sencilla el HTTP es el protocolo que gobierna los hipertextos a lo largo de la red y el código HTML crea y da formato a las páginas de un documento WEB. Para trabajar con un documento WEB el usuario debe ejecutar un software cliente llamado browser o navegador. Existen muchos ejemplos de navegadores como Netscape, Internet Explorer, Ópera, los cuales han transformado la Web en un medio interactivo que alberga texto con formato, gráficos, sonidos, imágenes y video.

CÓMO TRABAJA EL INTERNET

El Internet usa un Packet Switch Network tal como lo usa el servicio postal de los Estados Unidos de Norteamérica. El Internet transfiere información a través de una conexión que se realiza por medio de una línea telefónica cuando se hace la llamada utilizando el teléfono, una parte de la red es apartada o separada para el usuario que en ese momento realiza la conexión. Nadie de la red telefónica puede usar esta conexión que ha sido reservada por medio de la línea telefónica, es decir, cada usuario del Internet únicamente puede utilizar el espacio que le es proporcionado por la red y ese espacio nadie más lo puede utilizar.

El Internet, es como la oficina postal. El correo de cada usuario se mezcla con el de otros muchos, para después pasar por un filtro, que transfiere a la oficina postal y es ahí donde es ordenado y enviado al usuario o destinatario.

IV.- QUÉ ES EL CIBERESPACIO

Para poder entender qué es el ciberespacio, basta con imaginarnos un continente tan vasto que puede tener dimensiones infinitas. Es un mundo en el cual el usuario de la computadora puede llegar a una frontera electrónica llamada ciberespacio o espacio cibernético, en donde se guardan datos, se procesan y se mueven a través de vastas redes de comunicación; en donde los usuarios de las computadoras tienen acceso a diversas bases de datos, es decir, es la red de servidores de Internet. En otras palabras el ciberespacio no es otra cosa que el medio por el cual el Internet se desplaza o por el cual las personas que utilizan las computadoras se pueden comunicar entre sí hasta lugares muy distantes entre sí.

Y al igual que sucede con cualquier invento o descubrimiento nuevo, la domesticación del ciberespacio representa muchos retos y oportunidades para los usuarios de computadoras, profesionales de datos corporativos, empresarios de la informática y otros usuarios del mismo. Para tal efecto, es necesario redactar leyes para definir la

cualidades tan peculiares de posesión, propiedad y de valor que en el ciberespacio se dan. Así mismo, es de suma importancia el crear y desarrollar una ética que regule cómo se tratan entre sí los usuarios del ciberespacio o Internet, aceptándose los estándares para que podamos vivir en plena convivencia y seguridad entre los usuarios del ciberespacio e ir de la mano con la tecnología que siempre se encuentra cambiante.

V.- LA TRANSFERENCIA DE CRÉDITO A TRAVÉS DEL INTERNET O TRANSFERENCIA ELECTRÓNICA

Dentro del Internet, existe una serie de negocios que en un principio parecieran haberse tomado de una novela de ciencia ficción. Éstos van desde las conversaciones en directo (chatear) y videoconferencias, hasta la compra-venta de bienes muebles e inmuebles, esto último inclusive pagándose por medio de transferencias vía electrónica, ya sea con tarjetas de crédito o dinero virtual. En la actualidad, es un

hecho este tipo de negocios y es precisamente que las tarjetas de crédito y el dinero virtual son los medios por los que se concretan.

En nuestros tiempos, ya no es nada raro que las instituciones de crédito cuenten con varios servicios que se ofrecen mediante el Internet. Estos servicios van desde el pago de servicios con cargo a una tarjeta de crédito o cuenta de cheques, pasando por los depósitos del denominado dinero virtual a otras cuentas diferentes a las del usuario, consulta de saldos, hasta el pago de la nómina a los empleados de una empresa. A lo anterior, se le ha venido denominando “banca virtual” y en México el primer banco que ofreció sus servicios de banca virtual fue Banco IXE.

Como se comentó anteriormente, en Internet, las transacciones comerciales se realizan con tarjetas de crédito y el dinero virtual. Sin embargo, se buscan nuevas soluciones para la realización de las mismas, pues en principio la red de Internet no es segura. Así por ejemplo, si el programa de navegación que utilicemos contiene información sobre nuestra cuenta de crédito, llámese tarjeta de crédito

o cuenta de cheques, es muy probable que en ocasiones, comerciantes mal intencionados realicen cargos a ellas sin contar con nuestra autorización; o que al realizar un pago, nuestra información quede expuesta a ser interceptada y modificada, o inclusive para que se realicen otras compras no autorizadas por nosotros. Actualmente, se están buscando nuevas soluciones para esta clase de problemas de inseguridad en el intercambio de información de importancia, sólo basta recordar que la milicia norteamericana, abandonó el Internet por considerarla una red insegura.

Este problema toma dos vertientes, la primera es la autentificación, es decir, que los interlocutores sean en realidad quienes dicen ser, y la segunda, cuidar la privacidad e integridad de los datos que circulan, para que un tercero no pueda observar copiar o modificar el contenido de la información mientras se transmite.

Para esto se buscan las soluciones basadas en la criptografía digital, es decir, sistemas de cifrado que consisten en aplicar un método a la información que la convierta en texto cifrado, o sea que carece de

sentido a primera vista y sólo al aplicarle el método contrario, se obtiene la información original.

Otra de las soluciones propuestas se basa en firmas digitales, que son en sí un conjunto de datos que se añaden al contenido de una transmisión y que permiten que el receptor pueda comprobar la integridad de la información enviada y la veracidad de la fuente.

Las posturas que se han dado a este respecto son las de dos grandes consorcios que luchan por la supremacía en el sector y que son las siguientes:

- SEPP (Secure Electronic Payment Protocol) Postulado por Mastercard, GTE Corp. IBM, Netscape y Cibercash
- STT (Secure Transaction Technology) Lidereado por VISA y Microsoft

Cabe mencionar que ya ha sido lanzada la primera tarjeta de crédito para Internet con el nombre de “Web Master”, obviamente respaldada

por Mastercard, y que ya está en los medios gráficos de comunicación (vista por primera vez por el autor en Junio de 1996).

Para el mes de Julio de 1996 y como una clara muestra de la rápida evolución de la red, muchas páginas con servicios de venta ya aceptan pagos del banco “First Virtual”, y los sitios con Security sites abundan.

First Virtual

El First Virtual es el primer banco virtual dentro de la red para realizar transacciones comerciales y empezó a utilizarse desde el primer semestre de 1996; con este sistema se agilizan las transacciones comerciales. En México no es un sistema útil aún como sistema de cobro pero puede usarse como de pago. Según su Guía Internacional de Usuarios para ser comprador o vendedor, se requiere lo siguiente:

Compradores. Se requiere una tarjeta Visa o Mastercard que pueda aceptar cargo en dólares americanos (casi cualquier tarjeta

internacional alrededor del mundo lo hace). Cualquier cargo que se haga usando el sistema First Virtual será automáticamente convertido a la moneda local por la empresa que haya otorgado la tarjeta; como se puede apreciar, es como cualquier compra internacional que hayamos efectuado.

Vendedores. Para convertirse en vendedor se requiere una cuenta bancaria que acepte depósitos vía la United States Automated Clearing House (USACH). Los bancos que aceptan estos depósitos son todos los de los Estados Unidos Americanos. Sin embargo, sus sucursales en el extranjero generalmente, no aceptan este tipo de depósitos, sólo sus sucursales en los Estados Unidos, actualmente los bancos canadienses trabajan en aceptarlos.

Security Sites

Cuando no existe la posibilidad de depósitos automáticos, se recurre a sitios de seguridad (Security Sites). Estos son espacios dentro de los servidores en los que toda la información viaja encriptada, utilizando

software especial de seguridad, de manera que nadie puede observarla, ni modificarla. En este caso, el proveedor de servicios o en su caso el Webmaster (administrador de nuestro sitio) proporcionará una lista de las personas que realizaron compras y los datos necesarios para tramitar con nuestro banco, los cargos correspondientes.

Sistemas de encriptado y PGP

Mucho es lo que se ha dicho sobre la inseguridad de Internet, y muchos de los sistemas antes mencionados han sido víctimas de fraude al verse capturados y desencriptados sus paquetes de información por gente conocida como “hackers”. Sin embargo, los sistemas de encriptado han avanzado, convirtiéndose no sólo en una opción para el pago, sino en un medio de hacer privada la comunicación entre personas, lo que ha provocado una conmoción en las autoridades de varios países, incluso algunos que han manifestado una postura que se opone a la utilización u obtención de estos sistemas tales como Francia e Iraq, e incluso en países más progresistas como Estados Unidos.

El autor de uno de estos sistemas, Philip Zimmerman, creador del PGP (Pret Good Privacy), es actualmente acosado por el FBI y la CIA, y se ha generado una gran acción legal para conseguir la prohibición del programa que hasta la fecha ha fallado.

PGP (Pret Good Privacy)

PGP es un sistema de encriptación, cuya diferencia con los demás sistemas es que utiliza dos llaves para poder desencriptar el mensaje, una pública y otra privada, de manera que el emisor, solicitará la encriptación del mensaje (y consecuente conversión a números binarios para poder ser enviado), con la llave pública del receptor, que podrá ser enviada por un medio común (no encriptado) ya que esta llave sirve sólo para el encriptado y ni aún la persona que lo haya realizado puede abrirlo, pues se requeriría la llave privada para hacerlo y en muchos casos sólo se podrá hacer en la máquina en que se generaron las llaves.

Funciona mediante complejos algoritmos matemáticos, que dan como resultado un mensaje inexpugnable, razón por la que ha creado conmoción, pues las autoridades americanas protestan al no poder monitorear las comunicaciones por Internet, un punto con muy distintos enfoques. Por un lado, está el derecho a la privacidad, o acaso es necesario mirarnos cara a cara y revisar el lugar para saber que nuestro derecho es respetado. Y el otro enfoque, el de las autoridades, que temen que estos sistemas se puedan emplear para la transmisión de información ilegal, coordinación de este mismo tipo de actividades, o intercambio de información sensible como el diseño de bombas u otro tipo de armas.

Existen muchos sistemas de encriptado, pero existe también software que se encarga del proceso inverso, pero como ya se mencionó, el mensaje creado por PGP es inexpugnable, independientemente de que además se pueden agregar datos de validación como firmas.

Los que aún duden que sea posible la transmisión de información que deba ser totalmente segura, pienso que esta nota puede ser de ayuda para cambiar su parecer, los comentarios según Netguide:

Existen programas especiales para romper un e-mail encriptado, pero el PGP está diseñado de tal manera que según las estimaciones, una computadora utilizando mil millones de chips, cada uno de ellos mucho más poderoso que cualquiera que exista en la actualidad, requeriría de 10 billones de años, para tratar todas la posibles combinaciones generadas por uno solo de los algoritmos de encriptación usados en el PGP.

Hay otros programas de encriptación disponibles peor como el autor cita, “¿cuál es el que más molesto tiene al gobierno?”.

Seguramente en un futuro, se inventarán programas para desencriptar estos mensajes, o quizá llegue a prohibirse la utilización del PGP, pero no existe una manera de frenar el avance y si desea, la red puede ser

desde hoy un lugar seguro para efectuar transacciones comerciales de cualquier magnitud.

VI.- SU USO EN LA ACTUALIDAD

Hasta mediados de los años 60, las computadoras eran muy caras, máquinas de uso específico que sólo grandes instituciones como gobiernos y universidades podían pagar. Estas primeras computadoras eran usadas principalmente para realizar tareas numéricas complejas como hacer un cálculo preciso de la trayectoria de un cometa o algo por el estilo. Aunque las computadoras sí eran útiles para realizar este tipo de tareas, muy pronto fueron utilizadas para realizar otro tipo de tareas.

Fue IBM la empresa que en 1964 lanzó a la venta la macrocomputadora Sistema/360 de la cual llegó a comercializar aproximadamente 33,000, con exitoso resultado comercial, por este motivo los demás fabricantes de computadoras tuvieron que tomar

como modelo la computadora Sistema/360, para poder competir con IBM.

La empresa Digital Equipment Corporation en 1970 dio dos pasos gigantescos al introducir sus computadoras PDP-11 y VAX, las cuales venían en varios tamaños para satisfacer diferentes necesidades y presupuestos. Desde entonces, las computadoras han seguido reduciéndose y proporcionando más poder por menos dinero; hoy en día las computadoras de escritorio que se utilizan en oficinas y escuelas, cuentan con el poder suficiente para realizar diversas aplicaciones comerciales.

A la par del enorme crecimiento que han tenido las computadoras en los negocios, otros usos para ellas se han desarrollado con rapidez, actualmente se usan computadoras de todos tamaños y capacidades con propósitos que van desde la venta de boletos para eventos deportivos, culturales y recreativos, hasta para la administración de la nómina de una empresa.

En la actualidad no podríamos ver la modernidad de nuestra sociedad sin la existencia de las computadoras, no podríamos ver el avance en diversas ramas de la sociedad, como el caso de la economía, por poner solamente un ejemplo. Hoy en día, desde nuestra oficina hasta las operaciones bancarias, son una muestra de la relación que guardamos con las computadoras. No hay actividad en la que no tengamos algo que ver con las computadoras, hasta en el coche nos encontramos con una computadora que administra los recursos de nuestro vehículo.

Las computadoras se utilizan en la Medicina desde él diagnostico de las enfermedades hasta el monitoreo de los pacientes que se encuentran en terapia intensiva, para el seguimiento en las cirugías y el control permanente de trasplantes, e inclusive pequeñas computadoras que se implantan dentro del cuerpo humano con el propósito de ayudar al buen funcionamiento de algún órgano de vital importancia.

En la educación, el uso de la computadora se ha vuelto muy importante ya que actualmente se imparten clases a través del Internet,

siendo estas clases un complemento para la educación que se imparten en las aulas de las Universidades.

Los maestros están particularmente interesados en la computadora como una herramienta interactiva para el aprendizaje, ya que en contraste con los programas de televisión educativa que tenían que ser grabados, los programas de educación asistidos por computadoras, son capaces de solicitar retroalimentación del estudiante provocando de esta forma una respuesta en el momento, dándose de esta forma la interacción en el aprendizaje.

Por su parte, los científicos utilizan las computadoras para desarrollar teorías, recolectar y probar datos, así como para intercambiar datos con sus colegas alrededor del mundo. Los científicos e investigadores tienen acceso a diversas bases de datos en distintos lugares del mundo, todo con la ventaja de no tener que desplazarse a ningún lugar, ya que basta con tener una computadora conectada al Internet, para poder tener acceso a estas bases de datos. El espacio es un ejemplo donde la intervención de las computadoras es de suma importancia, tanto para

simular eventos complejos como el de las naves espaciales, hasta para transmitir datos a todo el mundo a través de los satélites.

En fin, el uso de las computadoras en la actualidad es sin lugar a dudas ilimitado y por consiguiente las leyes, así como las demás ciencias deben evolucionar y tomar en cuenta todos los alcances que tienen las computadoras; así como las implicaciones que el uso inadecuado o doloso de las mismas tiene para la sociedad.

CAPÍTULO SEGUNDO “LOS DELITOS QUE SE COMETEN POR MEDIO DE INTERNET”.

I.- EL CRIMEN COMPUTACIONAL

Muchas cosas que suceden en el espacio cibernético están más allá de la jurisdicción de las leyes tradicionales. Por ejemplo, cualquier persona hábil con una computadora puede navegar a través de una base de datos corporativa sin dejar rastro alguno, robarse datos sin que el dueño tenga conocimiento o infectar un sistema de cómputo con un virus de computadora que destruye información vital, además de que causa daños irreversibles al equipo de cómputo principalmente en el disco duro y memoria RAM.

Para lidiar con problemas como éstos, nuestro sistema legal no cuenta ni ha empezado a desarrollar o definir nuevamente las leyes que gobiernan la propiedad del software o de datos, violaciones a la propiedad ni tampoco ha adicionado las clases de delito que se pueden cometer. Éste es el primer paso para civilizar el espacio cibernético: la

creación de un juego estándar de reglas a través del cual se puede mantener un comportamiento aceptable.

En esta sección veremos la más apremiante de estas cuestiones legales, empezando con los dos problemas más importantes relacionados con software; el robo de software o el robo y los virus. Luego, pasaremos al tema cada día más importante del robo de hardware. Finalmente, exploraremos cómo se puede violar la propiedad de datos.

II.- ROBO DE PROGRAMAS (PIRATERÍA DE SOFTWARE)

El problema legal más importante, por mucho, que afecta a la industria de cómputo hoy en día es el robo del software, que es el copiado o uso ilegal de programas, sin el consentimiento del titular de los derechos. El robo de software es un problema enorme principalmente porque es muy fácil de realizar. En la mayoría de los casos, es tan difícil copiar un programa como grabar un CD que te ha prestado un amigo, los dos actos son ilegales.

Leyes de derechos de autor relacionados con el software.

Parte de la razón por la cual el robo de software es tan difícil de parar es que algunos tipos de copias se puede decir que son legales, un hecho que tienta a algunas personas a interpretar mal las diferencias. Por ejemplo, es generalmente legal hacer copias del software que le pertenece al usuario para que pueda tener una copia de respaldo en caso de que el original se dañe. Es más, instalar una nueva pieza de software significa copiar los programas del disco flexible al disco duro de la computadora y las instrucciones e instalación generalmente le indican que haga una copia de respaldo en otro juego de discos flexibles. Sin embargo, algunas compañías dicen que sólo puede tener los discos flexibles originales además de una copia instalada. Una vez que el programa está instalado, cada vez que se arranca le recuerdan la condición de derechos de autor.

Las compañías de software solían hacer sus programas con protecciones que impedían su copiado, pero eso dificultaba su instalación y hacer las copias de respaldo.

Por ejemplo, algunos discos de programas se hacían de tal manera que se pudieran copiar al disco duro del comprador sólo unas cuantas veces pero la mayoría de las compañías encontró que este tipo de protección contra copias causaba más problemas que los que resolvía,

Por poner un ejemplo, en Estados Unidos de Norteamérica, la mayoría de los desarrolladores hoy en día se respaldan en la ley y en el respeto de la gente a la ley. La ley principal que gobierna el robo de software en Estados Unidos es todavía la ley de Derechos de Autor de 1976. En 1983, se agregó una “Enmienda sobre el robo de software y copias ilegales”; más recientemente, el robo del software comercial fue elevada de ser un delito menor a ser un delito grave.

La justificación para estas leyes es que el software es propiedad intelectual, generalmente creada con la intención de hacer dinero. Las firmas comerciales de software varían en tamaño, desde un programador independiente hasta grandes corporaciones, tales como Lotus Development y Microsoft.

La creación de un programa complejo es un proceso extremadamente costoso que puede tomarle miles de horas a programadores muy entrenados. En los Estados Unidos de América tienen leyes en contra del robo de software, las cuales fueron creadas para proteger los intereses de las personas y las compañías que desarrollan software. Sin esta legislación, crear buen software podría no ser una buena inversión y, sin un buen software, le revolución del cómputo se acabaría.

Versiones de red y licencia para centros de cómputo.

Las empresas son los compradores más grandes de hardware y software. Como resultado, la pérdida potencial más grande de ingresos causada por el robo de software es de empresas y organizaciones que abusan de las leyes de derechos de autor.

La tentación es fuerte. Imaginemos a un maestro de secundaria con acceso a un laboratorio de cómputo de 25 computadoras. Quiere que sus estudiantes aprendan Lotus 1-2-3, pero a varios cientos de dólares por copia para cada computadora, su director nunca aprobará el gasto.

Por otro lado, podría comprar una sola copia del software y cargarlo en todas las computadoras del laboratorio, después de todo, es por una buena causa. El problema es que lo está haciendo sin el consentimiento del creador del programa.

Las organizaciones que tienen un grupo de computadoras y quieren correr el mismo programa en varias de ellas son muy comunes. Dado el potencial de pérdidas en ingresos causado por el robo de software, muchas compañías que desarrollan programas han adoptado la estrategia de vender licencias para centros de cómputo y versiones de red de sus programas.

Una **licencia para centros de cómputo** es un arreglo a través del cual el comprador de un programa compra el derecho de usarlo en determinado número de máquinas por menos del precio de compra de cada copia del programa para cada computadora.

Esencialmente, las licencias para centros de cómputo son una manera de que las compañías de software desanimen el robo del mismo ofreciendo un descuento por volumen.

Además de la copia única del software que viene con la licencia para el centro de cómputo, el comprador generalmente recibe varias copias de la documentación (el manual del software) y algunas veces servicios de soporte especiales de la compañía de software.

La **versión de red** es una variante de la licencia de centros de cómputo. Hoy en día, muchas compañías conectan todas sus computadoras en una red de área local (LAN). Los archivos que se necesitan por más de un empleado, especialmente los de bases de datos de una compañía, se almacenan en otra computadora llamada servidor de la red.

Frecuentemente, los programas que se usan también pueden ir en el servidor para que cada empleado no tenga que almacenar una copia separada en su disco; sin embargo, si la compañía compró sólo una

copia de uso único del programa (uno que le permita al comprador utilizar el programa en sólo una computadora a la vez), cargar el programa en el servidor de la red para que múltiples usuarios tengan acceso es robo.

Entonces, ¿qué debe de hacer la compañía? Obviamente comprar docenas de copias del programa sería un desperdicio. Una versión de red permite a la compañía comprar sólo una copia que pueda cargar legalmente en su red y permitir a algunos o a todos sus empleados usarla.

Al igual que una licencia para centros de cómputo, una versión de red generalmente, viene con varias copias del manual de software y soporte técnico especial de la compañía del software. Algunas versiones de red también incluyen características extras que las hacen más atractivas de lo que sería un acopia única que se ha pirateado.

Software de demostración o Shareware.

Otra estrategia para combatir el robo de software es el shareware, que es un software distribuido en forma gratuita para ser probado. Si el

usuario decide quedarse con el programa y seguir usándolo, debe pagar al desarrollador.

Normalmente, el shareware es desarrollado por compañías relativamente pequeñas o inclusive por programadores individuales, y generalmente es barato. El arreglo de shareware permite a los desarrolladores cargar programas en foros de información pública tales como boletines electrónicos, poniendo este software a la disposición de un gran número de clientes sin costo de ventas o de publicidad.

La lógica aquí es que ya que estos programas a menudo son más limitados en ámbito o atracción que los paquetes de software más comunes, es más fácil que la gente los copie ilegalmente antes de pagar su precio en la tienda. El arreglo de shareware trata de prevenir el robo poniendo el software en una situación de ética.

Software gratuito o Freeware.

Una respuesta final al problema del robo de programas es el freeware. Aunque sea difícil de creer, algunos programas son gratuitos. Ocasionalmente, la gente desarrolla programas para su propio uso y después los pone a la disposición de otra gente sin ningún costo.

En algunos casos, el desarrollador no reclama derechos de autor y el programa se convierte en software del dominio público, lo que quiere decir que cualquiera puede usar sin costo ni restricción. En otros casos, el software tiene derechos de autor pero el desarrollador le ha permitido a otra gente usarlos y copiarlo gratuitamente, aun cuando no sea del dominio público.

El lugar más común para encontrar programas gratuitos es en boletines electrónicos y servicios de información a través del Internet, en los que el desarrollador ha cargado una copia del programa en una base de datos compartida.

Generalmente, los programas de freeware no son aplicaciones complejas. Sin embargo, algunos son excelentes como por ejemplo, el programa llamado “messenger” que ofrece Microsoft, para escribirse en directo con otros usuarios de la página de Mircrosoft.

III.- VIRUS COMPUTACIONAL

Aunque el robo de software es con mucho el crimen computacional más predominante, uno igual de preocupante es la creación de virus computacionales.

Un ***virus***, en el ámbito de la computación, es un programa parásito oculto dentro de otro programa legítimo almacenado en un área especial del disco llamada *boot sector* (sector de arranque). Al ejecutar el programa legítimo o al accesar el disco se activa el virus, el cual puede estar programado para hacer muchas cosas, incluyendo copiarse a sí mismo en otros programas, mostrar información en la pantalla, destruir archivos de datos o borrar un disco duro completo. Un virus

puede incluso ser programado para mantenerse dormido por un tiempo específico o hasta cierto día.

El famoso virus Miguel Ángel, que causó un susto internacional en 1991, estaba programado para activarse el día del cumpleaños del artista. Cuando los usuarios prendieron sus computadoras infectadas ese día, el programa reformateó sus discos duros, borrando todos los datos y programas que estaban almacenados ahí.

En la actualidad los virus que han causado daños en las computadoras de varios consorcios han sido el “w32 o sircam”, “código rojo” (virus creado para afectar instituciones financieras así como a sus usuarios, el cual entró en funcionamiento a nivel mundial en noviembre del 2001) y “help (o ayuda)”.

Los científicos del área de la computación discutieron por primera vez la posibilidad de un programa capaz de duplicarse a sí mismo y extenderse entre las computadoras desde los 50. Pero no fue sino hasta 1983 que un software de virus real fue creado, cuando un estudiante en

la Universidad de California, Fred Cohen, escribió una tesis de doctorado sobre el tema.

Motivo para crear virus. A diferencia de los virus que causan resfriados y enfermedades en humanos, los virus de computadora no ocurren en forma natural, cada uno debe ser programado. No existen virus benéficos. Algunas veces son escritos como una broma, quizá para irritar a la gente desplegando un mensaje humorístico. En estos casos, el virus no es más que una molestia. Pero cuando un virus es malicioso y causa daño real, ¿quién sabe realmente la causa? ¿Aburrimiento? ¿Coraje? ¿Reto intelectual? Cualquiera que sea el motivo, los efectos pueden ser devastadores.

Prevención de infección. Afortunadamente, proteger un sistema contra virus no es tan difícil, con un poco de conocimiento y algo de software de utilería que se tenga a la mano. Lo primero que se necesita conocer es en qué momento corre peligro de infección un sistema. Una vez que está dentro de la memoria de la computadora, el virus puede destruir programas y archivos de datos en el disco duro.

La manera más común de pescar un virus de computadora es mediante el intercambio de programas o discos con otras personas. Aún programas comprados en paquetes sellados se ha sabido que han tenido virus.

La mejor precaución es tratar a todos los discos como portadores potenciales de infección.

Verificar si hay virus requiere de un software antivirus, el cual explora los discos y programas en busca de virus conocidos y los erradica. El uso de un programa antivirus es fácil. Una vez que está instalado en el sistema y activado, busca automáticamente archivos infectados cada vez que se inserta un disco flexible o se usa el módem para recuperar un archivo.

Existen algunos programas antivirus excelentes, algunos incluso son gratuitos. Una nota de precaución: constantemente están apareciendo nuevos virus, por lo cual ningún programa puede ofrecer una protección absoluta contra ellos.

IV.- ROBO DE LOS COMPONENTES FÍSICOS DE LA COMPUTADORA O HARDWARE

Los crímenes relacionados con el robo de programas y la creación de virus son muy conocidos y han recibido mucha publicidad. Pero el software (programas) no es la única parte vulnerable de la computadora. El robo simple es también un problema.

A pesar de que el robo de hardware ha ocurrido durante años, el problema no fue especialmente serio antes de que aparecieran las PC. Pero la introducción de la microcomputadora en los años 70 hizo que el equipo valioso fuera mucho más fácil de mover. El problema se disparó con la popularidad de las pequeñas computadoras portátiles.
Cuando microcomputadoras potentes con valor de varios miles de dólares pueden doblarse al tamaño de una hoja de papel tamaño carta y meterse en un portafolios, no es sorprendente que ocasionalmente desaparezcan.

El problema se agrava por el hecho de que la gente compra estas máquinas compactas para poder trabajar donde quiera que vaya. Cada día es más común ver a la gente usando computadoras en trenes, autobuses, aviones, hoteles y restaurantes. Es evidente que una computadora liviana de cuando menos 20 mil pesos en un aeropuerto concurrido no es un artículo seguro.

Las computadoras notebook y laptop son ahora objeto de hardware más robados, pero existen otros. También son robadas las microcomputadoras de las compañías, así como dispositivos periféricos como impresoras y módems.

Probablemente, una buena parte de este tipo de crimen es realizado por empleados de confianza. Aunque este tipo de crimen no es nuevo en los negocios, se convierte más en una amenaza a medida que los dispositivos caros continúan haciéndose más pequeños.

La moraleja es, desde luego, tomar precauciones. Muchas escuelas, negocios y otras organizaciones aseguran sus equipos de cómputo con

cables. Aun equipo relativamente barato, como los teclados, muchas veces se fija al escritorio o al resto de la computadora.

V.- ROBO DE INFORMACIÓN

Sorprendentemente, no sólo es robado el hardware de cómputo; particularmente en las empresas y en el gobierno, el robo de datos puede ser mucho más serio. Hay tres maneras en que los datos pueden ser robados. Primera, alguien puede llevarse el medio en que son almacenados los datos. Segunda, alguien puede robarse la computadora y su disco duro. Tercera, alguien puede entrar ilegalmente a los sistemas de cómputo de una organización y obtener acceso a archivos importantes.

Datos valiosos en las computadoras portátiles. Una vez más, es la introducción de poderosas computadoras portátiles lo que ha contribuido, al menos en parte, a este problema. A medida que ejecutivos de negocios, personal militar y funcionarios del gobierno se acostumbran a la conveniencia de traer cargando su computadora

donde quiera que van, también pueden poner en peligro la seguridad de los datos almacenados en sus máquinas.

En Estados Unidos de Norteamérica existen reportes de ladrones que ganan hasta 10 000 dólares por robarse la computadora portátil de un ejecutivo corporativo. El motivo en estos casos claramente no es la computadora en sí, ya que la mayoría de las portátiles no valen la mitad de esta cantidad. En vez de ésto, son los datos del disco duro de la computadora lo que es valioso.

Después de todo, el conocimiento de las estrategias que persigue un negocio para obtener ventaja sobre sus competidores, puede valer millones.

Lo que es peor, pensar en las implicaciones militares de un país que roba planes de defensa de otro o de las instrucciones de un presidente a un embajador al ser robada antes de una reunión muy importante.

Reconociendo el peligro que implica almacenar información importante en una computadora portátil, las organizaciones han

desarrollado varios métodos para protegerse. El más obvio es simplemente asegurar la computadora con un cable. Otra manera más sutil es programar una contraseña dentro del sistema operativo de la computadora. Aun para arrancar una computadora, el usuario debe teclear la contraseña correcta. Naturalmente, la protección con contraseña también puede ser usada para asegurar los datos de la computadora de escritorio. La protección con contraseña evita que personas no autorizadas puedan, por ejemplo, entrometerse en el disco duro de un ejecutivo del área de personal mientras él o ella se encuentre alejado de su computadora.

Quizá la forma más efectiva de seguridad es la *criptografía*, un proceso de codificación y descodificación de datos. La criptografía es usada con mayor frecuencia en los sistemas de mensajes como correo electrónico.

El método más común de criptografía, conocido como DES Digital Encryption Standard (Criptografía Estándar Digital), puede codificar un mensaje en más de 72 X 10^{15} maneras. Debido a que una llave

especial de software es utilizada para descifrar el mensaje, una intercepción no autorizada del mensaje no es una amenaza. En muchos sistemas de mensajes, se utiliza la criptografía DES aun cuando los usuarios no lo sepan.

VI.- EL DELINCUENTE CIBERNÉTICO O HACKER CRIMINAL

La otra manera en que se roban ocasionalmente los datos es por medio de un hacker, un programador muy hábil que se ha “descarriado”.

Abundan ejemplos muy coloridos de hackers criminales. Ladrones de tarjetas de crédito que utilizando una computadora personal se introdujeron subrepticiamente a una base de datos de TRW, compañía que guarda historiales de crédito, y pudieron tener acceso a registros confidenciales de crédito de 90 millones de personas.

Utilizando una computadora en su recámara, un estudiante de 17 años, de secundaria, se introdujo a la red de cómputo de AT&T y robó software con valor de 1 millón de dólares antes de ser descubierto.

Durante la campaña presidencial de los Estados Unidos de Norteamérica de 1992, una compañía arrendadora para consumidores obtuvo registros de crédito de varios trabajadores de la campaña de Ross Perot; según Equifax, compañía que guarda récords de crédito, la información vino de algunos hacker.

Alguien con habilidades de hacker también puede hacer el papel de héroe. Revisando una discrepancia de 75 centavos de dólar en una cuenta en el Laboratorio Lawrence Berkeley, un estudiante graduado llamado Clifford Stoll, rastreó a un intruso de cómputo a través de redes internacionales para descubrir un círculo de espionaje de alta tecnología. Las variantes y las posibilidades son ilimitadas.

Una acción del delincuente cibernético es sólo una variante computarizada del crimen de malversación (apropiarse de dinero o bienes fraudulentamente), por lo común de la empresa donde trabaja.

Los malversadores de cómputo son gente que manipula las cuentas computarizadas de una compañía para desviar fondos para su propio uso.

Los malversadores son difíciles de atraer, porque pueden robar sólo pequeñas sumas de dinero en un período prolongado de tiempo. Por ejemplo, un malversador bancario podría dar instrucciones al sistema de cómputo para meter el balance de todas las cuentas de cheques de los clientes después del tercer dígito de redondeo a la cuenta del malversador. Aunque la cantidad de cada transacción fraudulenta nunca sería más de 1/20 de centavo, multiplicar las entradas por varios millones de cuentas al día es significativo.

En los Estados Unidos de Norteamérica, los registros del FBI, muestran que mientras un ladrón de bancos roba un promedio de 1600 dólares por asalto, un malversador de cómputo roba un promedio de 600 000.

La mayoría de los sistemas de cómputo corporativos o gubernamentales en Estados Unidos de Norteamérica, utilizan medidas de seguridad para limitar el acceso a sus sistemas. Un método común es proporcionar códigos de identificación de usuario y contraseñas a empleados autorizados. Antes de que un empleado pueda obtener acceso (log on), o entrar a los archivos de una computadora, debe teclear un *código de identificación de usuario* que lo identifica en la computadora.

Generalmente, los empleados necesitan teclear una *contraseña (password)*, que es un código secreto para verificar la identidad de cada persona. Si el código de identificación del usuario o su contraseña de acceso no es igual al que tiene registrado la computadora en su software de seguridad, el usuario no podrá entrar al sistema.

En México el uso de contraseñas se ha empezado a emplear por una buena parte de las empresas y prestadores de servicios que cuentan con una página de Internet.

Los privilegios de acceso pueden variar para diferentes empleados, de esta manera el presidente de la compañía puede ver información como las ventas y los estados de resultados que no estarían disponibles para la mayoría de los trabajadores.

La forma de operar del delincuente cibernético o hacker es encontrar un código de acceso de alto nivel o una manera de darle la vuelta al procedimiento normal de entrada. Una vez que alcanza este objetivo, el delincuente está en libertad para explorar las bases de datos, robar datos valiosos e incluso archivos.

No existe una solución fácil al problema que representan los delincuentes cibernéticos. La seguridad de la información está siendo cada día más sofisticada, pero lo mismo sucede con los delincuentes.

En Estados Unidos de Norteamérica, aunque se pueden imponer fuertes penalidades para protegerse en contra de esta práctica, atrapar a un hacker criminal puede ser extremadamente difícil y los métodos

utilizados para hacerlo algunas veces implican una serie de dilemas éticos.

La búsqueda y detección de hacker sospechosos han resultado ocasionalmente en el arresto y acción judicial de gente involucrada en actividades perfectamente legales.

En 1990, después de una inexplicable caída de 9 horas de la red de larga distancia de AT&T, los agentes del servicio secreto arrestaron a Craig Neidorf, un estudiante universitario de Georgia que una vez había publicado en su boletín informativo electrónico, una copia ilícita de un documento de una compañía de teléfonos como un ejemplo divertido de proceso burocrático. Tiempo después, el caso del gobierno se desplomó cuando se descubrió que la información que Neidorf había publicado podía pedirse por aproximadamente 20 dólares.

Incidentes como éste han alarmado a la gente en relación con las libertades personales legales en la época de las comunicaciones

electrónicas. Un resultado ha sido la formación de la Electronic Frontier Foundation (EFF), por varios pioneros de la computación como Mitch Kapor, fundador de Lotus Development Corporation, y Steve Wozniak, mago de la computación y cofundador de Apple Computer.

Desde su fundación en 1990, EFF ha mantenido tres objetivos principales: investigación, desarrollo de políticas y servicios legales. En el área de investigación, EFF lucha por entender y mantenerse adelante en los desarrollos del campo de las computadoras. La EFF aboga por políticas públicas que promuevan la apertura en las comunicaciones. Finalmente, la EFF destina una gran parte de sus recursos a defender a usuarios de cómputo contra la aplicación excesivamente estricta de la ley.

Como hemos visto en los párrafos que anteceden, Estados Unidos de Norteamérica siendo un país desarrollado y que cuenta con leyes que regulan los ilícitos a través de Internet, cuenta con serios problemas. México que carece de la normatividad relativa con estos ilícitos, es

blanco fácil de la comisión de estos delitos que se llevan a cabo por medio del Internet.

Hoy en día además de los delitos que se indican en el presente capítulo, en México me ha tocado constatar los siguientes:

1.- Compraventa de bienes simulados.

El caso que a un servidor tocó, consistió en que un programador, desarrolló un portal o página de venta de computadoras utilizando el nombre comercial de un fabricante de equipos de cómputo de renombre. En el portal creado por el delincuente, ponía a la venta varios modelos de computadoras y la forma de adquirir el modelo por parte de las personas interesadas en su compra, era solamente mediante el pago con tarjeta de crédito y el llenado de un formato que contenía los espacios para los datos del comprador como: nombre, dirección, tipo de tarjeta de crédito y número de la misma, así como la fecha de vencimiento de ésta. El ilícito se daba una vez que el comprador de la computadora llenaba con sus datos el formato, ya que

nunca recibía la computadora adquirida. Sin embargo, en el estado de cuenta de su tarjeta de crédito se cargaba el importe correspondiente a la computadora y al tratar de cancelar o aclarar la compra ante el banco emisor de la tarjeta, ésta no procedía en virtud de que efectivamente se había adquirido una computadora con el importe que se le cargaba en su estado de cuenta. Además de que aparecía su consentimiento en la página del prestador de servicios en donde el delincuente había adquirido la computadora. Es decir, que los datos proporcionados al comprar una computadora en la página de Internet falsa, fueron los que utilizó el delincuente en una página de Internet debidamente establecida.

Después de haberse realizado una investigación por parte del banco, éste determinó que la compra no se podía cancelar en virtud de que la página de Internet en donde ingresó el tarjeta habiente fue cancelada o eliminada del servidor que se utilizó para desarrollar la página de Internet falsa.

2.- Transferencias bancarias ficticias, delictuosas y reales.

Ficticias. Son aquellas en las que el delincuente cibernético concreta al argumentar que cuenta con los fondos suficientes y en el caso concreto del que tuve conocimiento, sucedió cuando en una operación de compraventa de antigüedades en donde un supuesto comprador acudió a las oficinas del vendedor de antigüedades y una vez que se pusieron de acuerdo en el precio de compra de las antigüedades, el comprador le propuso al vendedor la forma de pago por medio de una transferencia electrónica a nombre del vendedor y al acceder este último, el comprador le pidió utilizar el Internet de la oficina para realizar la transferencia del dinero, con la salvedad de que para poder realizar dicha transferencia, el comprador insertó un disco compacto o CD con el que explicó al comprador que era necesario para ingresar al banco donde tenía su cuenta, así que lo insertó. En realidad lo que contenía el CD era un programa que simulaba entrar a la red de un determinado banco y aparentaba realizar y confirmar operaciones vía transferencia electrónica, pero en ningún momento se tenía conexión real con el banco. En el caso que comento, una vez que corrió el

programa el delincuente y el comprador ante sus propios ojos confirmó la transferencia electrónica del dinero e hizo entrega de las antigüedades. El comprador tuvo conocimiento de la transferencia ficticia al girar un cheque de la cuenta a la que supuestamente se le había hecho el depósito y éste fue devuelto por carecer de los fondos suficientes.

CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

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

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

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).

d) Lectura, sustracción o copiado de información confidencial.

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

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

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

h) Uso no autorizado de programas de cómputo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

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

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a los dispositivos de almacenamiento.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

a) Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b) Los que utilizan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

c) Los que utilizan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

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

a) Acceso no autorizado: es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo

electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

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

c) Interceptación no autorizada: en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

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

Clasificación del delito informático de Siebert Ulrico, profesor alemán de la Universidad de Würzburgo, clasifica la criminalidad informática basándose no sólo en la tipología delictiva que demuestra los distintos tipos de delitos que pueden cometerse, si no también en los campos de estudio que genera la problemática del delito cometido por medios informáticos, clasificándolos de la siguiente manera:

a) Protección de la privacidad: en donde lo que busca es la protección de la información personal de datos por medio de computadoras, incluyéndose normas penales para proteger la privacidad, esto surgió en los años 70 y principios de los 80 en países como Alemania, Suecia y Estados Unidos.

b) Delitos económicos.- comienza en 1980, como reacción a la legislación criminal tradicional que protegía exclusivamente los bienes materiales o tangibles frente al desarrollo de bienes intangibles, nuevos soportes informáticos y el surgimiento de dinero electrónico. El proceso legislativo comienza en los Estados Unidos en 198, extendiéndose a Europa en la última década.

c) Protección de la propiedad Intelectual: aunque este tipo de delitos tiene una relación con los anteriores por su importancia económica, tomando en consideración a los programas de computación como obras protegidas por el derecho de autor, en 1980 con la protección para semiconductores y en 1990 para las bases de datos y los secretos industriales y comerciales.

d) Contenido ilegal y nocivo en las autopistas de la información: señala que en el Internet es posible encontrar todo tipo de información, y en especial aquella de contenido discriminatorio para minorías, o el caso de pornografía infantil.

e) Derecho procesal penal: ha sido reformado en diversos países para combatir el crimen organizado con nuevas tecnologías o permitir que el mismo este a la par de la técnica.

f) Derecho y Seguridad: es el ultimo grupo de cuestiones que comenzó a discutirse a partir de 1990 relativo a la creación de requisitos y prohibiciones de medidas de seguridad, por ejemplo el

uso de criptografía; o los medios empleados para sobrepasar una protección técnica de algún derecho de bienes intangibles.

CAPÍTULO TERCERO “LOS DELITOS POR INTERNET”

I.- CONCEPTO DEL DELITO

En primer lugar y a fin de entender objetivamente lo que es un delito, es necesario definirlo, para posteriormente continuar con los elementos del mismo, como lo son: la conducta, el tipo o hecho, la antijuridicidad, culpabilidad y en último término, la punibilidad.

Así, en este orden de ideas tenemos que el delito es y, a lo largo de los tiempos, ha sido entendido como una valoración *jurídica*, objetiva o subjetiva, la cual encuentra sus precisos fundamentos en las relaciones necesarias surgidas entre el *hecho humano* contrario al orden ético-social y su especial estimación legislativa.

Los pueblos más antiguos castigaron los hechos objetivamente dañosos y la ausencia de preceptos jurídicos no constituyó un obstáculo para justificar la reacción punitiva del grupo o del individuo lesionado contra su autor, fuera éste un hombre o una bestia. Sólo con el transcurso de los siglos y la aparición de los cuerpos de leyes

reguladores de la vida colectiva, surgió una valoración *subjetiva* del hecho lesivo, limitando al hombre a la esfera de aplicabilidad de la sanción represiva.

Diversas ramas del conocimiento humano, se han ocupado de estudiar al delito entre otras se han ocupado la Filosofía y la Sociología. La primera de estas ciencias a estimado al delito como una violación de *un deber, necesario para el mantenimiento del orden social, cuyo cumplimiento encuentra garantía en la sanción penal*, mientras la segunda lo identifica como una *acción antisocial y dañosa*.

Al respecto el afamado jurista GARÓFALO, estructura un concepto de ***delito natural***, viendo en él *una lesión de aquella parte del sentido moral, que consiste en los sentimientos altruistas fundamentales como lo son la piedad y la probidad, según la medida media en que son poseídos por una comunidad y que es indispensable para la adaptación del individuo a la sociedad*. Tal concepto fue objeto de merecidas y justificadas críticas. Aunque GARÓFALO trató de encontrar algo común al hecho ilícito en todos los tiempos y lugares,

de manera que no estuviera sujeto a la constante variedad de su estimativa según la evolución cultural e histórica de los pueblos, su empeño quedó frustrado, pues su concepto del delito resultó estrecho e inútil.

Por su parte el autor CARRARA, con su concepto de "ente jurídico" distinguió al delito de otras infracciones no jurídicas y precisó sus elementos más importantes. Lo consideró como "*la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso*". De esta definición destaca, como esencial, que el delito es una *violación a la ley*, no pudiéndose concebir como a cualquier otra no *dictada precisamente por el Estado*, con lo cual separa, definitivamente, la esfera de lo jurídico de aquellas otras pertenecientes al ámbito de la conciencia del hombre, precisando su naturaleza penal, pues sólo esta ley se dicta en consideración a la *seguridad* de los ciudadanos.

II.- **CONCEPTO JURÍDICO DEL DELITO**

Para definir al delito en términos jurídicos, en algunos Códigos se ha pretendido dar una definición del delito, como en el del Distrito Federal, en el cual se le hace consistir en el *acto omisión que sancionan las leyes penales*, tal concepto es puramente formal al caracterizarse por la amenaza de sanción a ciertos actos y omisiones, otorgándoles por ese único hecho el carácter de delitos.

Un concepto *substancial* del delito sólo puede obtenerse, dogmáticamente, del total ordenamiento jurídico penal. De éste desprendemos que el delito *es la conducta o el hecho típico, antijurídico, culpable y punible*, afiliándonos, por tanto, a un criterio *pentatómico*, por cuanto consideramos son cinco sus elementos integrantes:

a) una conducta o un hecho
b) la tipicidad
c) la antijuricidad

d) la culpabilidad, y

e) la punibilidad

ASPECTOS NEGATIVOS DEL DELITO

La moderna doctrina jurídico-penal considera que a cada elemento del delito corresponde un aspecto negativo, el cual impide su integración.

ELEMENTOS	ASPECTOS NEGATIVOS
Conducta o hecho	Ausencia de conducta o de hecho
Tipicidad	Atipicidad
Antijuricidad	Causas de justificación
Culpabilidad	Inculpabilidad
Punibilidad	Excusas absolutorias

LA PRELACIÓN LÓGICA ENTRE LOS ELEMENTOS DEL DELITO

Celestino PORTRE PETIT precisa la inexistencia de *prioridad temporal* entre los elementos del delito, en virtud de que éstos concurren simultáneamente, al no perderse de vista su indisoluble unidad. Asimismo, niega la *prioridad lógica*, pues la existencia del delito requiere de sus elementos y, aunque ellos guardan entre sí un determinado orden lógico, no hay ninguna prioridad lógica. Lo correcto, según su opinión que nosotros compartimos, es hablar de *prelación lógica*, "habida cuenta de que nadie puede negar que, para que concurra un elemento del delito, debe antecederle el correspondiente, en atención a la naturaleza propia del delito. La circunstancia de que sea necesario que exista un elemento para que concurra el siguiente, no quiere decir que haya *prioridad lógica*, porque ningún elemento es fundante del siguiente, aún cuando sí es necesario para que el otro elemento exista.

III.- EL HECHO Y SUS ELEMENTOS. LA CONDUCTA

EL HECHO COMO DELITO Y COMO ELEMENTO DEL DELITO.

El delito es un fenómeno fáctico jurídico que tiene realización en el mundo social. Por tal efecto, en el campo del Derecho penal, se identifica al término **"hecho"** con el delito mismo, dándosele, igualmente, un significado y connotación diversos, en sentido restringido como elemento del delito.

Así, por ejemplo, con referencia al homicidio, se dice que es el hecho consistente en la privación violenta de la vida, estimándolo no sólo en cuanto a su significación objetiva sino ligándolo al autor de los hechos; pero ya cuando se habla en concreto del delito de homicidio, al *hecho* se le estima como aquel conjunto de elementos materiales que se encuentran descritos en el tipo que sanciona la privación de la vida.

DEFINICIÓN Y ELEMENTOS DEL HECHO

El jurista JIMÉNEZ DE ASÚA, adopta el vocablo *acto,* para denominar el elemento fáctico del delito, es congruente cuando afirma que por tal debe entenderse en tal virtud define al hecho como "*la manifestación de voluntad que mediante acción produce un cambio en el mundo exterior, o que, por no hacer lo que se espera deja inerte este mundo externo, cuya mutación se aguarda*".

Asimismo define que la conducta "es siempre una *manifestación de voluntad* dirigida hacia un fin".

JIMÉNEZ DE ASÚA concluye que, se hable de acto o bien de conducta, que son elementos de uno o de otra, la *manifestación de voluntad* y el *resultado,* elementos que se unen, en relación de causa y efecto, por la existencia del *nexo causal*.

CONCEPTO DE CONDUCTA COMO ELEMENTO DEL HECHO

Por regla general los autores, al abordar este problema, tratan de dar un concepto sobre la conducta haciendo referencia a las dos formas en que puede expresarse el proceder humano, es decir, aludiendo tanto a la *actividad* como a la *inactividad* del sujeto. En tal virtud, LÓPEZ FALLO sostiene: " La conducta es una actividad voluntaria o una inactividad voluntaria (o no voluntaria en los delitos culposos por olvido), que produce un resultado con violación: a) de una norma prohibitiva, en los delitos comisivos; b) de una preceptiva en los omisivos; y c) de ambas, en los delitos de comisión por omisión".

Así las cosas estimamos que, la conducta consiste en el peculiar *comportamiento* de un hombre que se traduce exteriormente en una *actividad* o *inactividad voluntaria.* El concepto anterior, es comprensivo de las formas en las cuales la conducta puede expresarse: *acción u omisión*.

Cabe mencionar que, la conducta consiste exclusivamente en una *actividad o movimiento corporal*, o bien en una *inactividad, una abstención, un no hacer*; tanto el actuar como el omitir, el hacer como el no hacer, tienen íntima conexión con un factor de carácter psíquico que se identifica con la *voluntad de ejecutar la acción o de no realizar la actividad esperada.*

IV.- LA TIPICIDAD

CONCEPTO DEL TIPO

Para el caso del estudio de la tipicidad, segundo elemento del delito, hace necesario previamente el análisis del tipo para precisar su concepto y su contenido.

Concepto de Tipo, en sentido amplio, se considera al delito mismo, a la suma de todos sus elementos constitutivos, concepto al que hicieron referencia, como vieja acepción del término.

Por su parte otros autores aluden a la palabra *tipo*, en el sentido de la teoría general del Derecho, como "*el conjunto de todos los presupuestos a cuya existencia se liga una consecuencia jurídica*".

En un sentido más restringido y limitado al Derecho Penal, el tipo ha sido considerado como el conjunto de las características de todo delito para diferenciarlo del *tipo específico* integrado por las notas especiales de una concreta figura de delito.

El *tipo legal*, dándole connotación propia jurídico penal, es la *descripción concreta hecha por la ley de una conducta a la que en ocasiones se suma su resultado, reputada como delictuosa al conectarse a ella una sanción penal*. Tal concepto es diverso al de *tipicidad.*, al cual damos parcialmente, significado idéntico al de *adecuación típica.*

El carácter *concretizador de lo injusto*, por parte del tipo, ha sido observado de antiguo, razonándose en el sentido de que el legislador sólo crea los tipos penales configurando conductas estimadas "posible

mente antijurídicas", pues carecería de sentido formular tipos en donde se recogieran conductas indiferentes o neutras.

Así, se dice que el tipo penal *concreta* lo injusto, por ser éste anterior a aquél; lo antijurídico *precede en el tiempo* a su descripción.

TIPICIDAD Y ATIPICIDAD

En cuanto la tipicidad, estamos de acuerdo con la objeción hecha al empleo del término *tipicidad*, pero no podemos por este hecho, tomar como consideración general, en nuestro medio, como *adecuación típica*, supuesta la existencia del tipo legal o figura del delito.

En tal virtud, se entiende por *Tipicidad*, dado el presupuesto del tipo, que define en forma general y abstracta un compromiso humano, *la adecuación de la conducta o del hecho a la hipótesis legislativa;* "el encuadramiento del hecho en la figura legal", de tal manera que la tipicidad presupone el *hecho tipificado más la adecuación típica* del hecho concreto al tipo legal.

Sin embargo, no debe confundirse el tipo con la tipicidad; el primero es el antecedente necesario del delito, es decir, su *presupuesto*, mientras la *tipicidad* es uno de sus elementos constitutivos. Tal situación ya ha sido observada por nuestros penalistas, entre quienes Fernando Castellanos le otorga carácter de elemento esencial, pues su ausencia impide la configuración del delito. "No debe confundirse el tipo con la tipicidad -advierte-. El tipo es la *creación legislativa*; es la descripción que el Estado hace de una conducta en los preceptos penales. La tipicidad es la *adecuación de una conducta concreta con la descripción legal formulada en abstracto*".

V.- LA ANTIJURICIDAD

En el lenguaje jurídico penal los términos antijurídico, injusto e ilícito han venido siendo empleados indistintamente, dándoseles idéntica significación conceptual. A tal concepto, Guillermo SAUER destacó el mayor contenido de lo *injusto* con relación a lo *antijurídico.*

CONCEPTO

Desde la antigüedad se ha afirmado que la antijuridicidad es un concepto negativo, *desaprobador del hecho humano frente al derecho*.

Algunos autores, siguiendo un criterio que atiende a la ley, han pretendido dar una noción de la antijuridicidad en forma negativa. Así, PORTE PETIT argumenta que se tendrá como antijurídica una conducta adecuada al tipo cuando *no se pruebe la existencia de una causa de justificación.*, haciendo el comentario que hoy en día, así funcionan los códigos penales, valiéndose de un procedimiento de exclusión, lo cual significa en su criterio, la concurrencia de una doble condición para tener pro antijurídica la conducta: la violación de una norma penal y la ausencia de una causa de justificación.

Si no se pierde de vista que el hecho humano debe ser necesariamente *conforme* al Derecho o *contrario* a él, resulta cierto lo anteriormente afirmado, pero ese razonamiento nada nos dice sobre el concepto de lo antijurídico y menos aún sobre su contenido.

En general, los autores se muestran conformes en que la antijuridicidad es un desvalor jurídico, una contradicción o desacuerdo entre el hecho del hombre y las normas del Derecho.

Es antijurídica una acción cuando contradice las normas del Derecho. En tal virtud, la doctrina se encuentra acorde en considerar a la objetividad del injusto como un juicio de valor acerca de la relación entre el hecho y la norma de Derecho lesionada.

VI.- LA CULPABILIDAD

Hemos venido insistiendo que el delito es la conducta o hecho típico antijurídico, *culpable* y punible, confirmando así lo precisado por la mayor parte de los autores contemporáneos: la culpabilidad es un elemento constitutivo del delito; sin él no es posible concebir su existencia. Tal verdad quedó como antecedente, mismo que fue utilizado por el jurista BELING al elaborar el principio “nulla poena sine culpa”, cuyo rango es fundamental en el Derecho penal moderno.

En *amplio sentido* la culpabilidad ha sido estimada como "*el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica*", comprendiendo por ello a la imputabilidad, mientras en *sentido estricto*, otros estudiosos del derecho penal sostienen que la *culpabilidad es reprochabilidad*, calidad específica de desvalor que convierte el acto de voluntad en una acto culpable.

ELEMETOS DE LA CULPABILIDAD

El desarrollo actual de la teoría normativa ubica, dentro del concepto de culpabilidad y por tanto como sus elementos, los siguientes:

I.- La *imputabilidad*.

II.- Las *formas de culpabilidad*, dolo y culpa, consideradas por algunos, como partes integrantes de la culpabilidad, que constituyen la referencia psíquica entre la conducta o hecho y su autor, y

III.- La *ausencia de causas de exclusión de la culpabilidad*, pues de existir una de ellas desaparecería la culpabilidad del sujeto.

Por su parte, la teoría psicológica da a la imputabilidad el carácter de *presupuesto* de la culpabilidad y fija el contenido de ésta en el punto *hecho psicológico,* por cuanto en él yace la necesaria relación entre la acción antijurídica y su autor.

LAS FORMAS DE LA CULPABILIDAD

EL DOLO

Tradicionalmente se han aceptado, como formas de culpabilidad, al *dolo* y a la *culpa*.

Una fuerte corriente de doctrina, ha visto en el *delito preterintencional* "una mixtura de dolo y culpa", fenómeno observado de tiempo atrás, iniciando la tendencia al reconocimiento que caracteriza a los bien conocidos delitos preterintencionales, ubicados por la mayoría dentro de la familia de los delitos dolosos.

TEORÍAS SOBRE EL DOLO

El *dolo*, la principal forma de culpabilidad, constituye tal vez el escollo más fácil de salvar en el estudio de la teoría del delito, pues en la elaboración de su concepto unos apoyan el elemento *psicológico* en la voluntad, mientras otros lo hacen en la *representación*, en tanto el elemento *ético* se pretende fundamentar en el conocimiento de la *tipicidad del hecho*, o de su *antijuridicidad*, o bien en la *conciencia del quebrantamiento del deber*, lo cual viene a poner de relieve la existencia de diversas teorías en formulación de su concepto.

TEORÍA DE LA REPRESENTACIÓN Y DE LA VOLUNTAD EN FORMA VINCULADA

Una postura ecléctica adopta esta teoría para la cual no basta a integrar el dolo ni la voluntad ni la sola representación, siendo ambas indispensables. En consecuencia, de acuerdo con ella, actúa dolosamente quien no sólo ha representado el hecho y su significación

sino además encamina su voluntad, directa o indirectamente, a la causación del resultado.

En esta posición, hay quienes empiezan por afirmar el necesario conocimiento del hecho en sí y en sus efectos, así como su contradicción con la ley, dándose en esas condiciones la inteligencia que prepara el discernimiento, lo cual lleva al sujeto a determinarse, fenómeno apoyado tanto en la voluntad como en la libertad externa.

Para otros, el que obra dolosamente prevé y quiere el delito (en la totalidad de sus elementos: acción y resultado, antijuridicidad y culpabilidad), concepto aceptado por la definición del Código italiano (artículo 43, apartado primero), siendo por consiguiente dos los elementos del dolo:

1) La previsión (o representación del resultado).
2) La volición de él.

"No basta la previsión sin la voluntad, pero tampoco basta la voluntad sin la previsión. La previsión sin la voluntad es vana; la voluntad sin previsión es ciega; y el derecho no puede contentarse con ninguna de las dos… *Previsión* es la representación del resultado y denota el momento intelectivo de la conducta… *Voluntad* es el acto de autodeterminarse en vista de algún fin. *Querer* es tender a un objeto y a un fin (presentes en la conciencia y por esto representados) y obrar e consecuencia…"

LA TEORÍA ACEPTABLE

La última de las teorías examinables es, a nuestro criterio, la correcta. Hemos de recordar en este lugar la conclusión adoptada al examinar el coeficiente psíquico de la conducta. En su oportunidad dijimos que la *voluntad* constituye dicho coeficiente, el cual consiste en querer realizar la acción o la omisión, o bien la voluntad de no inhibir el movimiento corporal o la inactividad.

Ahora bien, la voluntad en el dolo rebasa el estrecho ámbito de la conducta para abarcar igualmente el resultado, de manera que si la

voluntad en la conducta consiste en querer realizar la acción o la omisión, *la voluntad en el dolo es querer también el resultado.* En el homicidio, el coeficiente psíquico de la conducta consistirá en querer realizar la acción (disparar = movimiento corporal) o la omisión (no dar al enfermo el medicamento prescrito = inactividad), en tanto dicha voluntad en el dolo radicará en querer o aceptar el producir la muerte que se sabe consecuencia de la propia acción u omisión.

La voluntad, por si misma, no puede agotar el contenido del dolo; hácese imprescindible igualmente el conocimiento de las circunstancias del hecho y de su significación. Tal conocimiento debe abarcar la relación de causalidad, cuando ésta forma parte del hecho particularmente tipificado; la tipicidad del mismo, entendida de manera profana, y su carácter antijurídico.

LAS FORMAS DE LA CULPABILIDAD

LA CULPA

La experiencia diaria nos demuestra cómo en ocasiones la conducta humana, no proyectada voluntariamente a la producción de un daño, lo origina causalmente. En tales situaciones afirmarse la existencia de culpa cuando la actitud del sujeto, enjuiciada a través del imperativo de los deberes impuestos por la ley, es reprochable a virtud de la inobservancia de la prudencia, atención, pericia, reglas, órdenes, disciplinas, etc., necesarias para evitar la producción de resultados previstos en la ley como delictuosos.

Cuando se trata de establecer la noción de la culpa, acudiendo a la opinión de los doctos, es fácil extraviarse por los muy diversos senderos a que conducen las variadas concepciones elaboradas sobre ella. Hácese por tanto imprescindible el examen de lagunas de las principales teorías sobre la culpa, para iluminar un tanto el camino que nos lleve a al determinación de su concepto.

LA TESIS QUE CONSIDERAMOS MÁS ADECUADA

En la formulación del concepto de culpa entran diversos ingredientes de naturaleza bien diversa. No podemos en manera alguna prescindir de la previsibilidad como tampoco del deber de cuidado exigido por la ley al punir determinadas consecuencias de la conducta humana.

La voluntad tiene importancia referida concretamente a la acción o inacción del sujeto, pero no debe conectarse con el evento dañoso. El carácter evitable del acontecimiento luctuoso juega igualmente importante papel en la culpa.

En todo acontecimiento culposo se incumple un deber, más no el deber de observancia de la norma prohibitiva que sanciona el resultado típico y antijurídico, sino de otro diverso formulado implícitamente en la obligación de abstenerse. El sujeto debe limitar sus actos a las actividades o inactividades que no rebasen la línea abstracta que conduce a la creación de un peligro, pues con ello está infringiendo un especial deber descuidado o una prohibición expresa impuesta por la ley, la costumbre o la razón.

LOS ELEMENTOS DE LA CULPA

De lo anteriormente expuesto surgen como elementos de la culpa los siguientes:

a) *Una conducta voluntaria* (acción u omisión), reconocida unánimemente, pues sólo del hecho producido por la acción u omisión voluntarias puede originarse un juicio de culpabilidad.

b) *Un resultado típico y antijurídico.* Al referirnos a la culpabilidad dejamos establecido que el juicio en que se hace consistir el elemento subjetivo del delito, presupone necesariamente un hecho típico y antijurídico, lo cual significa que el acontecimiento sobrevenido, en nexo causal con la acción u omisión, se adecua perfectamente al hecho comprendido en un tipo penal y que el mismo resulta contrario a la norma en el juicio objetivo de valoración.

c) *Nexo causal entre la conducta y el resultado.* No puede prescindirse de este elemento en la formulación del concepto de culpa. Para poder

atribuir el resultado al agente se precisa la relación causal de la conducta con aquél.

d) *Naturaleza previsible y evitable del evento.* Sólo tomando en cuenta la previsibilidad y evitabilidad del resultado puede fundamentarse la violación de los deberes de cuidado impuestos por la ley y la sana razón, pues a nadie puede reprochársele su incumplimiento si el evento era imprevisible e inevitable.

e) *Ausencia de voluntad de resultado.* Sin discusión alguna, el delito culposo excluye la posibilidad de la voluntad del sujeto respecto al resultado. En él no existen intención delictiva, ya por falta de previsión o por la esperanza de que le mismo no sobrevendría.

f) *Violación de los deberes de cuidado.* La obligación del sujeto de cumplir con el deber de cuidado genera, al realizar la conducta contraria que implica su violación, la responsabilidad culposa cuando con ello se produce el resultado.

CLASES DE CULPA

La culpa se clasifica en *consciente*, llamada también con representación o previsión e *inconsciente,* denominada igualmente sin representación o sin previsión.

Existe *culpa consciente* cuando el sujeto ha representado la posibilidad de causación de las consecuencias dañosas, a virtud de su acción o de su omisión, pero ha tenido la esperanza de que las mismas no sobrevengan.

La *culpa inconsciente* (sin representación) es cuando el sujeto no previó el resultado por falta de cuidado, teniendo obligación de preverlo por ser de naturaleza previsible y evitable.

VII.- LA PUNIBILIDAD

Al definir el delito expresamos que un concepto substancial del mismo sólo puede obtenerse, dogmáticamente, del total ordenamiento jurídico y de éste se desprende que pro tal debe entenderse la conducta o el hecho típico, antijurídico, culpable y punible. Dimos por tanto, a la punibilidad, el tratamiento de carácter fundamental o elemento integral del delito.

Desde un punto de vista formal el concepto del delito puede reducirse, como lo dejamos precisado antes, a la conducta punible (acto u omisión que sancionan las leyes penales), según lo determina el artículo 7 del Código Penal.

Por *punibilidad* entendemos, *la amenaza de pena que el Estado asocia a al violación de los deberes consignados en las norma jurídicas, dictadas para garantizar la permanencia del orden social*.

CASTELLANOS TENA, congruentemente con su punto de vista de considerar a la punibilidad como una consecuencia del delito, precisa que se habla de *ausencia de punibilidad* cuando, realizado un delito, la ley no establece la imposición de la pena, haciendo con tal expresión referencia a los casos en los cuales, dada la existencia de una conducta típica, antijurídica y culpable, el legislador, por motivos de política criminal, basada en consideraciones de variada índole, excusa de pena al autor. *"Así entendida, la ausencia de punibilidad opera cuando el ordenamiento jurídico establece de manera expresa excusas absolutorias"*.

CAPITULO CUARTO “PROPUESTAS RESPECTO A LOS DELITOS COMETIDOS POR INTERNET”

I.- CONCEPTO DE DELITO INFORMÁTICO

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

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".

Para Carlos Sarzana, en su obra Criminalita e Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

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

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española".

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 en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

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

Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

a) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

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.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

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.

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 último recurso para evitar su impunidad.

II.- CARACTERÍSTICAS DEL 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 habilidades 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 sinnúmero de conductas que considera como delitos de cuello blanco, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

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 sí 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.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales

diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

III.- CARACTERÍSTICAS DEL SUJETO PASIVO

En primer término tenemos que 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 crediticias, gobiernos, etc., 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 mantengan 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 e 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.

El único antecedente con el que cuenta nuestra legislación, en el que se contempla al delito informático es el CÓDIGO PENAL DEL ESTADO DE SINALOA. Ante la importancia que tiene este delito el Congreso Local del Estado de Sinaloa ha legislado sobre el particular, en cuyo texto se menciona.

"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.

Es claro 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.

Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda

mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

CONCLUSIONES

Hoy día nuestro código Penal Federal, el cual nació el 14 de agosto del año de 1931, no contempla reglas especificas sobre los delitos cometidos por medio de la computadora, medios electrónicos e informáticos. No es difícil imaginar que en el año de creación de nuestro Código penal, las computadoras y demás medios electrónicos, no existían, ni mucho menos la tecnología que actualmente es utilizada por millones de personas en forma diaria.

Después de identificar al delito informático, a través del presente trabajo, así como de la revisión detallada de nuestra legislación vigente, hemos determinado aquellas carencias que presenta nuestra legislación en materia informática.

Apoyándonos en el derecho comparado observamos claramente dos tendencias con respecto de la legislación dictada en materia de delitos informáticos. La primera de ellas consiste en la creación de leyes especiales, en donde se contemplen varios artículos donde se creen lo

nuevos tipos o delitos informáticos e incluso se legisle sobre algunas cuestiones específicas como ser la competencia o el significado de los términos usados en las normas. Se enrolan en esta corriente Portugal, Chile, Alemania, Estados Unidos en algunos caso, e Inglaterra.

La otra tendencia que encontramos en esta materia es la reforma del Código Penal mediante la inserción de nuevos tipos penales o la modificación de los existentes para adaptarlos a las nuevas tecnologías. Han seguido esta variante entre otros Italia, Canadá, Austria, Francia y algunas leyes estatales de Estados Unidos.

Por mi parte, considero que lo pertinente es modificar un tipo penal ya existente, pero ubicándolo dentro del capítulo correspondiente del Código Penal. Ello trae consigo la ventaja de que se crea una nueva figura a la que se le da autonomía en su formulación y se facilita así la interpretación del nuevo delito, dentro del capítulo en el cual se encuentra y en función del bien jurídico que se intenta proteger, pues como decía Sebastián Soler: “la determinación del bien jurídico tutelado es la mejor guía para la correcta interpretación de la ley”

Cabe mencionar que nuestro Código posee diferentes títulos cada uno corresponde en general a la idea de reunir todas las figuras que afecten determinado bien jurídico, aunque dentro de cada título las figuras a su vez se distribuyen en fragmentaciones del bien jurídico genérico.

En este orden de ideas las conclusiones propuestas son las siguientes:

1.- Se propone la reforma del Código Penal Federal, para aceptar los avances tecnológicos, en especial los delitos informáticos.

2.- Reformar también el Código de Procedimientos Penales, para permitir combatir con eficacia y eficiencia al delito informático.

3.- Preparar a los elementos que integran las fuerzas policiales e investigación, con el equipamiento y conocimiento necesario en materia informática.

4.- Que el tipo de delito informático sea contemplado por el Código Penal Federal, ya que tiene que ser de competencia Federal y no local.

5.- En algunos casos se deben tomar soluciones específicas teniendo en cuenta las diferencias existentes entre la propiedad tangible y la intangible. Esto es importante respecto de la información, que es un nuevo bien jurídico que no puede ser tratado de la misma forma en que se aplica la legislación actual a los bienes corporales.

6.- Se requieren nuevas normas jurídicas que tengan en cuenta al autor de la información, al tenedor, a la persona a la cual se relacionan esos datos y a la protección de la sociedad contra los contenidos ilícitos.

7.- Elaborar medidas especificas para combatir el crimen, sobre todo respecto del crimen organizado y de las complejas formas delictivas de hoy en día, que incluyen lavado de dinero y los fraudes a los negocios financieros, que con el desarrollo de las redes informáticas van a adquirir una nueva dimensión.

Respecto al Código Penal Federal son necesarias las siguientes propuestas para adaptarlo a la actual realidad informática en particular lo siguiente:

a.- Incluir el fraude informático, como tipo especial en el Código Penal Federal, teniendo en cuenta que se trata de una modalidad donde a partir de datos o información falsa se obtiene la prestación de un bien o servicio administrado en forma automatizada a través del uso de una computadora.

b.- Incluir el daño informático, no sólo en la modalidad de destrucción de información (daño material) sino también en el daño lógico es decir la alteración o retraso en el funcionamiento de un sistema y la modalidad de denegación de servicio, para efectos de reparación del daño que se haya causado.

c.- Adicionar el daño causado en la propiedad intelectual en software, programas y derechos de autor en obras literarias, así como en el Código Penal Federal.

d.- Anexar como bien jurídico dentro del Código Penal Federal a la privacidad y a los demás derechos personalísimos y a las diversas formas de afectación que existen.

e.- Tipificar como delito el acceso ilegítimo a sistemas informáticos sean privados o públicos, así como el uso o tratamiento ilegítimo de esta información.

f.- Tipificar la interrupción del normal funcionamiento de sistemas informáticos y en especial las comunicaciones por medios electrónicos así como los ataques que puedan considerarse como terrorismo cibernético, sean ésstos daños en sistemas públicos o privados.

g.- Señalar el concepto de documento electrónico o firma digital dentro del Código Penal Federal, a fin de que se prevean lo delitos

específicos relacionados con la firma digital basada en la criptografía de clave pública.

h.- Las nuevas tecnologías permiten controlar al individuo en forma más eficiente, obtener información en forma automática y un seguimiento de sus acciones. Por ende, se debe extremar el análisis para evitar la violación de las garantías constitucionales.

i.- El uso de las tecnologías puede ayudar a combatir el crimen y a descubrir la verdad histórica, por ende su uso legítimo debe ser adoptado por las fuerzas de seguridad, y fomentada a través de la capacitación del personal de la Procuraduría General de la Republica y de la Suprema Corte de Justicia de la Nación.

j.- Lo planteado en el presente trabajo, puede ser visto desde muchos puntos de vista, dentro de los cuales algunos pueden o no coincidir, lo importante del mismo ha sido tratar de analizar brevemente la situación de la protección de la ley penal a todos los usuarios de los

medios informáticos, cibernéticos e Internet, para que no sean afectados en su patrimonio e intimidad.

k.- Por regla general, la legislación penal, por su territorialidad es pensada únicamente en función del propio territorio, pero para el caso del Internet y su aplicación en el ciberespacio, debe contemplarse en forma amplia para una efectiva aplicación, para tal efecto se requiere que sean considerados como delitos del ámbito Federal y por consiguiente mediante una reforma en el Código Penal Federal se adicionen lo delitos informáticos.

l.- Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática, como en el caso de la Corte Penal Internacional.

m.- Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, inteligencia artificial, redes), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

n.- Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de las computadoras.

o.- Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

p.- Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente

incremento de esta situación, es necesario a pesar de que en nuestro país el delito informático no ha alcanzado el grado de peligrosidad existente en esos Estados, regular penalmente las conductas ilícitas derivadas del uso de la computadora.

q.- En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

r.- Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, se sugiere que en el Título Vigésimo Segundo sobre los Delitos en Contra de las Personas en su Patrimonio del Código Penal Federal se añada un capítulo especial para los delitos informáticos.

s.- Teniendo en cuenta también la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos, como sería la analogía.

t.- Teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha sido el único que ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, se establece que es necesario que con objeto de que se evite un conflicto de competencia entre los Congresos Locales y el de la Unión, éste, con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros

elementos, la jurisdicción Federal y local de estos ilícitos, a fin de que sea únicamente el Código Penal Federal quien tipifique a los delitos informáticos y por consiguiente sean los Jueces federales Penales quienes conozcan de estos delitos, de conformidad a lo establecido en el articulo 50 de la Ley Orgánica del Poder Judicial de la Federación.

u.- Entiendo que en este nuevo mundo relacionado con el espacio, las conductas ilícitas no se tratan de un nuevo tipo de delitos sino que estamos ante formas delictivas novedosas que plantean una serie de inconvenientes a resolver, pero que no llegan a presentar la entidad suficiente desde el punto de vista conceptual y dogmático. Para comenzar, no se distingue un bien jurídico tutelado que le pueda ser adjudicado como propio o al menos principal. ¿Es la información, la propiedad, la intimidad, el dato, los sistemas informáticos en sí mismos, la seguridad y/o la fe pública?

Más bien podríamos incluir estas situaciones dentro de los ilícitos económicos y, más precisamente, dentro de la modalidad de “delitos de cuello blanco”, ya que es necesario contar con el conocimiento

técnico en informática, cibernética, para poder efectuar los delitos a través de Internet mediante el uso de computadoras.

v.- Al decir que no tienen suficiente entidad dogmática no se pretende desconocer su capacidad de daño en la sociedad, desde el punto de vista económico. Precisamente es esa capacidad dañosa la que más ha llamado la atención de penalistas y criminólogos, junto con algunas peculiaridades sociológicas del sujeto activo, las dificultades de descubrir las maniobras delictivas, su fácil encubrimiento, la cifra negra, y la rapidez de acción.

Entiendo, sin embargo, que aún no estamos ante una nueva categoría delictiva, sino ante la irrupción de un nuevo medio de un nuevo mecanismo tecnológico que ha hecho tambalear el sistema penal de la sociedad.

w.- La aplicación de tipos preexistentes a fenómenos tecnológicos innovadores y revolucionarios, no es nueva en la historia del Derecho

Penal. Ha sucedido por ejemplo, con la energía eléctrica y con la utilización de aparatos mecánicos.

La irrupción del automóvil, si bien generó nuevas situaciones de peligrosidad, no ha requerido la creación de tipos “ad hoc” en la mayoría de las legislaciones que siguen manteniéndose en sus tipos tradicionales.

x.- Para un sector de la doctrina, la violabilidad de la dignidad de la persona a través de medios informáticos, crea un nuevo derecho fundamental denominado indistintamente "Libertad Informática", "Derecho de autodeterminación informativa" o "Derecho a la Intimidad Informática". Cada una de estas denominaciones obedece al origen y posición doctrinal o jurisprudencial que se sigue para estructurarla. En cambio, considero junto a otro sector de la doctrina, que no existe un nuevo derecho sino una ampliación del contenido del derecho a la intimidad, evidenciada, por un lado, por la irrupción de las nuevas tecnologías de la información y de la comunicación en el mundo del derecho, generando entre otros aspectos, la informática jurídica entendida básicamente como ciencia del tratamiento lógico,

incardinado y cualificado de la información por medios informáticos, electrónicos y telemáticos; y por otro, cuando se considera a la intimidad como el derecho que tiene toda persona al control de la información de sí mismo (The Right to control information about oneself), cuando sus datos personales han sido sometidos a tratamiento informatizado. Este es sólo el comienzo de ya larga data sobre la irrupción de la informática al mundo del derecho o tal vez el intento del derecho de desembarcar en la informática.

B I B L I O G R A F I A

1.- ACEVEDO BLANCO, RAMON, “MANUAL DE DERECHO PENAL”, EDITORIAL THEMIS, COLOMBIA, 1983.

2.- ACOSTA ROMERO, MIGUEL, “DELITOS ESPECIALES”, EDITORIAL PORRUA, MÉXICO, 1990.

3.- ACOSTA ROMERO, MIGUEL, “LEGISLACIÓN BANCARIA”, EDITORIAL PORRUA, MÉXICO 1989.

4.- ANTOLISEI, FRANCESCO, “LA ACCION Y EL RESULTADO EN EL DELITO”, EDITORIAL JURÍDICA MEXICANA, 1959.

5.- BEEKMAN, GEORGE, “COMPUTACIÓN E INFORMATICA HOY”, EDITORIAL IBEROAMERICANA, 1995.

6.- CARRANCA Y TRUJILLO, RAUL, “DERECHO PENAL MEXICANO”, EDITORIAL PORRUA, MÉXICO, 1980.

7.- CARRANCA Y TRUJILLO, RAUL, ”CÓDIGO PENAL ANOTADO”, EDITORIAL PORRUA, MÉXICO, 1999.

8.- CASTELLANOS, FERNANDO, “LINEAMIENTOS DEL DERECHO PENAL”, EDITORIAL PORRUA, MÉXICO, 1982.

9.- CORREA, CARLOS M., “DERECHO INFORMATICO”, DEPALMA, BUENOS AIRES, 1992.

10.- COUTURE, EDUARDO L., “VOCABULARIO JURÍDICO”, EDICIONES DE PALMA, BUENOS AIRS, 1991.

11.- CRUMLISH, CHRISTIAN, “DICCIONARIO DE INTERNET BILINGUE”, EDITORIAL MC GRAW HILL.

12.- DICCIONARIO JURIDICO MEXICANO, INSTITUTO DE INVESTIGACIONES JURÍDICAS, MÉXICO, 1997.

13.- ENCICLOPEDIA DE INFORMATICA Y COMPUTACIÓN, PUBLICACIONES CULTURAL, MADRID, 1997.

14.- FALCON, ENRIQUE M., "¿QUÉ ES LA INFORMATICA JURÍDICA?", ABELEDO PRET EDITORES, BUENOS AIRES, 1992.

15.- GONZALEZ QUINTANILLA, JOSE ARTURO, "DERECHO PENAL MEXICANO", EDITORIAL PORRUA, MÉXICO, 1991.

16.- HANCE, OLIVER, "LEYES Y NEGOCIOS EN INTERNET", EDITORIAL MC GRAW HILL, 1996.

17.- HARRIS, L. MARTÍN, "INTRODUCCIÓN AL PROCESAMIENTO DE DATOS", EDITORIAL LIMUSA, MEXICO, 1976.

18.- ISLAS, OLGA, "LA LOGICA DEL DELITO EN EL DERECHO PENAL", EDITORIAL JURÍDICA, MEXICO.

19.- JIMÉNEZ HUERTA, MARIANO, "LA ANTIJURIDICIDAD", EDITORIAL PORRUA, MÉXICO.

20.- JIMÉNEZ HUERTA, MARIANO, "LA TIPICIDAD", EDITORIAL PORRUA, MÉXICO.

21.- LEGISLACIÓN BANCARIA, EDITORIAL PORRUA, MÉXICO, 1999.

22.- LEGISLACIÓN PENAL, EDICIONES ANDRADE, MÉXICO, 1999.

23.- LEY DE INSTITUCIONES DE CREDITO, EDITORIAL DELMA, MÉXICO, 1999.

24.- LEY GENERAL DE ORGANIZACIONES Y ACTIVIDADES AUXILIARES DEL CRÉDITO, EDITORIAL PORRUA, MÉXICO 1998.

25.- MARQUEZ PIÑERO, RAFAEL, “DELITOS BANCARIOS”, EDITORIAL PORRUA, MÉXICO, 1996.

26.- ORELLANO WIARCO, OCTAVIO ALBERTO, “CURSO DE DERECHO PENAL”, EDITORIAL PORRUA, MÉXICO, 1999.

27.- PORTE PETIT, CELESTINO, “PROGRAMA DE LA PARTE GENERAL DEL DERECHO PENAL”, EDITORIAL UNAM.

28.- TÉLLEZ VALDES, JULIO, “CONTRATOS INFORMATICOS”, EDITORIAL UNAM, MÉXICO.

29.- TÉLLEZ VALDES, JULIO, “DERECHO INFORMATICO”, EDITORIAL MC GRAW HILL, MÉXICO, 1990.

30.- TORRES LOPEZ, MARIO ALBERTO, “LAS LEYES PENALES”, EDITORIAL PORRUA, MÉXICO, 1993.