349

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGON

ESTUDIO ANALITICO DE LA NORMATIVIDAD DEL DELITO INFORMATICO ENTRE LA LEGISLACION NACIONAL Y LA LEGISLACION INTERNACIONAL

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

GABRIELA ORTIZ SALGADO

ASESOR: LIC. JOSE HERNANDEZ RODRIGUEZ

MEXICO 2001

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.

GRACIAS, DIOS POR PERMITIRME TENER UNA FAMILIA Y AMIGOS QUE SIEMPRE ME APOYARAN INCONDICIONALMENTE. GRACIAS, DIOS POR PERMITIRME VIVIR CADA DÍA CON TU BENDICIÓN. GRACIAS, DIOS POR PERMITIRME LLEGAR A ESTA ETAPA DE MI VIDA. A TÍ SEÑOR MÍO Y A MIS PADRES, LES DEDICO ESPECIALMENTE ESTA TÉSIS.

A MIS PADRES:
ALFONSO Y TARCILA, LES AGRADEZCO SU APOYO, SUS SACRIFICIOS, SUS EZFUERZOS Y TODO AQUELLO QUE HICIERON CON AMOR PARA QUE LOGRARA CONCLUIR MI CARRERA. POR TODO ESTO Y POR MUCHO MÁS GRACIAS..... GRACIAS POR SU AMOR.

A MIS HERMANOS:
PAULINA Y DAVID, POR ESA INFINITA TOLERANCIA QUE ME PRESTARON EN EL MOMENTO PRECISO Y POR SU COMPRENSION DE HERMANOS, GRACIAS.

A MIS ABUELITOS:
LUPITA(+) Y SANTIAGO, JUVENAL Y VIRGINIA, QUE POR SU TIEMPO Y POR SUS SABIOS CONSEJOS ME HAN FOMENTADO PRINCIPIOS Y VALORES, ILUMINANDO CON AMOR Y CARIÑO EL CAMINO DE LA VIDA. GRACIAS Y QUE DIOS LES DE SALUD ETERNA.

A MI NOVIO MAURICIO:
POR TU INFINITO AMOR, POR TU COMPRENSION Y PACIENCIA, PERO SOBRE TODO POR ESE APOYO QUE INCONDICIONALMENTE SIEMPRE ME HAS OFRECIDO, GRACIAS..... GRACIAS POR SER UNO DE MIS PRINCIPALES MOTIVOS PARA SEGUIR EN ESTA LUCHA. GRACIAS POR ESTAR SIEMPRE A MI LADO. QUE DIOS TE PROTEGA HOY Y SIEMPRE.
TE AMO

A MIS AMIGOS Y DEMAS FAMILIARES.
POR EL APOYO Y AMOR QUE SIEMPRE ME HAN BRINDADO A LO LARGO DE MI VIDA ACADÉMICA, GRACIAS. GRACIAS POR ESA AMISTAD INCONDICIONAL.

MI UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO, CAMPUS ARAGÓN:
QUE ME ABRIÓ SUS PUERTAS PARA PERMITIRME CREAR UNA FORMACIÓN ACADÉMICA Y PROFESIONAL INTEGRAL, HEREDANDO ASÍ ESE ORGULLO DE SER UNIVERSITARIO POR ESE PRIVILEGIO, A TI UNIVERSIDAD, GRACIAS.
¨ POR MI RAZA HABLARÁ EL ESPÍRITU ¨

A MIS PROFESORES:
POR SUS ENZEÑANZAS TAN VALIOSAS QUE ME SERVIRÁN TANTO PARA MI VIDA ACADÉMICA COMO EN LA PERSONAL. GRACIAS... GRACIAS POR ESA EDUCACION QUE ES COLUMNA VERTEBRAL DE TODO PROFESIONAL.

A MI ASESOR DE TÉSIS, LIC. JOSÉ HERNÁNDEZ RODRÍGUEZ:
POR HABER BRINDADO PARTE DE SU TIEMPO, CONOCIMIENTO Y SABIDURÍA, EN LA ELABORACIÓN DEL PRESENTE TRABAJO DE INVESTIGACIÓN.

ESTUDIO ANALÍTICO DE LA NORMATIVIDAD DE LOS DELITOS INFORMÁTICOS ENTRE LA LEGISLACIÓN NACIONAL Y LA LEGISLACIÓN INTERNACIONAL

I N D I C E

Introducción 1

CAPITULO I

ANTECEDENTES

1.1 Historia de la informática... 3

1.2 Antecedentes del delito informático.. 6

1.3 Inicios de la regulación de la informática 40

CAPITULO II

CONCEPTO DE DELITO Y DEFINICIONES DE DELITO INFORMÁTICO

2.1 Definición de delito y de delito informático.. 53
a) Sujeto Activo
b) Sujeto Pasivo

2.2 Clasificación de los delitos informáticos..... 61

2.3 Tipos de los delitos informáticos.... 66

CAPITULO III

MARCO JURÍDICO

3.1 Título Noveno y Vigésimo Sexto del Código Penal Federal.... 78

3.2 Ley Federal del Derecho de Autor..... 86

3.3 Sexta parte, Capítulo XVII, del Tratado de Libre Comercio de América del Norte..... 90

CAPITULO IV

ESTUDIO ANALITICO Y COMPARATIVO ENTRE LA LEGISLACION NACIONAL Y OTRAS LEGISLACIONES INTERNACIONALES

4.1 Otras legislaciones internacionales como los son Argentina, Alemania. Austria, Francia, Chile. Gran Bretaña, Holanda, Estados Unidos y España. 104

4.2 Lagunas existentes dentro de la legislación mexicana. 113

4.3 Necesidad de la creación de una Ley que regule y sancione los delitos informáticos..... 117

Conclusiones..... 122

Bibliografía..... 124

INTRODUCCIÓN

El fenómeno social de la tecnología informática ha llegado a rebasar las limítrofes de la imaginación humana, generando un importante número de conductas nocivas que aprovechando el poder social que la informática adquirió, buscan lucros ilegítimos causando daños y situaciones que han provocado la existencia y la creación de grupos organizados para el desarrollo de actos de dudosa legalidad apoyados en un sistema de cómputo.

En este orden de ideas se puede observar que la informática puede ser la mejor aliada o la peor enemiga del hombre, dependiendo del uso que a está se le dé, por lo que se ha llegado a afirmar que el derecho es la única forma efectiva para evitar la alteración de la paz cibernética.

Así pues, el objetivo del presente trabajo de investigación es realizar un estudio analítico y comparado de la legislación mexicana, que en la actualidad se encuentra regulando escuetamente actos relacionados con el acceso no autorizado a programas de cómputo y situaciones similares; y de las legislaciones internacionales que desde hace un par de décadas han regulado los delitos informáticos, con la intención de prevenir las consecuencias que por más desastrosas se han presentado en los países como España, Alemania, Estados Unidos y Francia entre otros.

Es por ello la importancia de realizar dicho estudio, con el propósito de encontrar la forma adecuada y práctica de regular las inevitables consecuencias que con el uso indebido de las computadoras y de los sistemas informáticos se han producido creando así los delitos informáticos, mismos que no han sido tipificados como tales en el Código Penal Federal, y que, como se mencionó y se señaló anteriormente, sólo sancionan conductas derivadas de los accesos ilícitos a sistemas computacionales y demás conductas. Inclusive, ni en el ordenamiento antes citado

ni en la Ley Federal de Derechos de Autor se señala que ordenamiento o ante que autoridad se deberá seguir el procedimiento legal específico.

Por lo que es importante y necesario, dado la naturaleza del tema de investigación, explicar la trascendencia que ha tenido la evolución de la informática a lo largo de la historia tecnológica en la humanidad. Exponiendo sin duda alguna el significado que tienen los delitos informáticos para los conocedores en la materia ya que es imprescindible conocer y tener referencia de los lineamientos y limitantes que puede alcanzar en la práctica esta área en el mundo jurídico. .

De tal manera que es inevitable referir el marco jurídico existente en nuestro sistema legal. señalando y explicando las referencias dadas en la materia de la informática en algunos artículos del Código Penal Federal y otros más de la Ley Federal de Derecho de Autor, implicados estos ordenamientos gracias a la recomendación dada en el Tratado de Libre Comercio de América del Norte celebrado entre nuestro país, Estados Unidos y Canadá.

Nos apoyaremos en los métodos inductivo, deductivo e histórico, para la realización y el desarrollo de la presente investigación.

La finalidad de esta investigación obedece a dos motivos, el primero es el de analizar el delito informático, para poder comprender sus alcances y sus consecuencias, de tal manera que podamos usar esta herramienta para la regulación de este delito y así poder proponer algunos cambios para su disminución y para que sea sancionado y castigado. El segundo motivo por el cual se esta realizando esta investigación, es para obtener el Título de Licenciado en Derecho.

CAPITULO I ANTECEDENTES

1.1 Historia de la Informática

Por siglos, los hombres han tratado de usar fuerzas y artefactos de diferente tipo para realizar sus trabajos, para hacerlos más simples y rápidos. La historia conocida de los artefactos que calculan o computan, se remonta a muchos años antes de Jesucristo.

EL ÁBACO

Dos principios han coexistido con la humanidad en este tema Uno es usar cosas para contar, ya sea los dedos, piedras, conchas, semillas etc. El otro es colocar esos objetos en posiciones determinadas. Estos principios se reunieron en el ÁBACO, antiguo instrumento de cálculo que aparece en diferentes partes del mundo especialmente en China y Japón en el año 2600 A C. Instrumento que sirve hasta el día de hoy, para realizar complejos cálculos aritméticos con enorme rapidez y precisión.

REGLA DE CALCULO

En el siglo XVII en Europa Occidental se encontraba en uso la **regla de cálculo**, calculadora basada en las invenciones de Nappier, Gunther y Bissaker. John Nappier (1550-1617) descubre la relación entre series aritméticas y geométricas, creando tablas que el llama logaritmos. Edmund Gunter se encarga de marcar los logaritmos de Nappier en líneas. Bissaker por su parte coloca las líneas de Nappier y Gunter sobre un pedazo de madera, creando de esta manera la regla de cálculo. Durante más de 200 años, la regla de cálculo es perfeccionada, convirtiéndose en una calculadora de bolsillo, extremadamente versátil. Así, por el año 1700 las calculadoras numéricas digitales, representadas por el ábaco y las calculadoras análogas, es decir, personificadas por la regla de cálculo, eran de uso común en toda Europa.

LA PASCALINA

Blasie Pascal además de escribir tratados filosóficos, literarios, científicos y matemáticos, se dio tiempo para inventar máquinas. En 1642 inventó una máquina de calcular, capaz de realizar sumas y restas. Aquel dispositivo utilizaba una serie de ruedas de diez dientes en las que cada uno de los dientes representaba un dígito del 0 al 9. Las ruedas estaban conectadas de tal manera que podían sumarse números haciéndolas avanzar el número de dientes correcto. Pese a su ocasional inexactitud, esta temprana **máquina de Pascal**, llegó a ser el prototipo de los artefactos calculadores, que se encuentran profusamente repartidos por todo el mundo.

LA CALCULADORA UNIVERSAL

El filósofo y matemático alemán Gottfried Wilhelm Leibniz creó un prototipo **de máquina calculadora** mecánica en 1671 y que con mejoras perfeccionó y terminó en 1694. Su artefacto se basó en el principio de la suma, multiplicación y división.

LA MÁQUINA DIFERENCIAL Y LA MÁQUINA ANALÍTICA

El profesor de matemáticas de la Universidad de Cambridge, Inglaterra, Charles Babbage (1792-1881), desarrolla en 1823 el concepto de un artefacto, que él denomina " **máquina diferencial** ". La máquina estaba concebida para realizar cálculos, almacenar y seleccionar información, resolver problemas y entregar resultados impresos. Babbage imaginó su máquina compuesta de varias otras, todas trabajando armónicamente en conjunto: los receptores recogiendo información; un equipo transfiriéndola; un elemento almacenador de datos y operaciones; y finalmente una impresora entregando resultados. Pese a su increíble concepción, la máquina de Babbage, que se parecía mucho a una computadora, no llegó jamás a construirse. Los planes de Babbage fueron demasiado ambiciosos para su época. Este avanzado concepto, con respecto a la simple calculadora, le valió a Babbage ser considerado como el precursor de la computadora. La prometida de Babbage, Ada Augusta Byron, luego Condesa de Lovelace, hija del poeta inglés Lord Byron, le ayudó en el desarrollo del concepto de la Máquina

Diferencial. creando programas para la máquina analítica, siendo reconocida y respetada, como el primer programador de computadoras. Un lenguaje de computación lleva hoy en día su nombre "ADA ".

LA MÁQUINA TABULADORA

El siguiente en aportar algo al moderno concepto de las computadoras, para seguir adelante fue el industrial francés Joshep Jackquard (1752-1834). Jackquard tuvo la idea de usar tarjetas perforadas para manejar agujas de tejer, en telares mecánicos. Un conjunto de tarjetas constituían un programa, el cual creaba diseños textiles. Una ingeniosa combinación de los conceptos de Babbege y Jackquard, dan origen en 1890 a un equipo electromecánico, que salva del caos a la Oficina de Censo de Estados Unidos. Hermann Hollerith usa una perforadora mecánica para representar letras del alfabeto y dígitos en tarjetas de papel, que tenían 80 columnas y forma rectangular. La máquina tabuladora de Hollerith, utilizaba corriente eléctrica para detectar los agujeros que estaban perforados y así hizo registrar la información en tarjetas, y el tiempo total se redujo Hollerith terminó asombrosamente su experimento, el cual fue un éxito. De esta forma fundó una compañía privada, la Tabulating Machine Co., donde en 1900, tras perfeccionar su invento a distintos modelos, la máquina alcanzaba la capacidad de procesamiento de 300 tarjetas por minuto. En 1911 se unen dos empresas más, formando así la Computer Tabulating Recording Co. Pero en el año de 1924 la empresa C.T.R. Co. pasó a llamarse definitivamente IBM (International Business Machines) para reflejar su presencia mundial.

LA COMPUTADORA ELECTROMÉCANICA MARK I

En 1944 se pone en funcionamiento la primera computadora al modo actual. Es el Doctor Howard Aiken en la Universidad de Harvard, Estados Unidos, quien la presenta con el nombre de Mark I. Es esta la primera máquina procesadora de información. La Mark I funcionaba eléctricamente, las instrucciones e información se introducen en ella por medio de tarjetas perforadas. Los componentes trabajan basados en principios electromecánicos. A pesar del peso superior a 5 toneladas

y su lentitud comparada con los equipos actuales, fue la primer máquina en poseer todas las características de una verdadera computadora.

LA COMPUTADORA ELECTRÓNICA ENIAC

La primera computadora electrónica se terminó de construir en 1946, por John W Mauchly y John Presper Eckert en la Universidad de Pensilvania, Estados Unidos y se llamó ENIAC. Con ella se inicia una nueva era, en la cual la computadora pasa a ser el centro del desarrollo tecnológico, y genera una profunda modificación en el comportamiento de las sociedades.

1.2 Antecedentes del Delito Informático

Como más adelante se explicará con detenimiento y con un escrupuloso estudio, los delitos informáticos se manifiestan en diferentes tipos, de acuerdo al acto realizado y a las consecuencias que éste conlleva, esta clasificación se encuentra reconocida por la Organización de las Naciones Unidas.

" Los principales tipos son: 1) Fraudes cometidos mediante manipulación de computadoras. Entre este tipo se encuentran la manipulación de los datos de entrada, la manipulación de los datos de salida; 2) Falsificaciones informáticas como objeto y como instrumentos; 3) Acceso no autorizado a servicios y sistemas informáticos; 4) Piratas informáticos o Hackers; 5) La Reproducción no autorizada de programas informáticos de protección legal y 6) Daños o modificaciones de programas o datos computarizados como lo es el sabotaje informático a través de los virus, gusanos y la bomba lógica. " [1]

Es en el transcurrir del tiempo y de los sucesos como la historia nos va dando elementos para estudiarla, para analizarla y entender el por qué de los acontecimientos. De esta manera, por el desarrollo de los acontecimientos es como obtenemos la no tan abundante historia de los delitos informáticos, dado que la

[1] Naciones Unidas Octavo Congreso de las Naciones Unidas sobre Prevencion del Delito y Tratamiento del delincuente La Habana, 27 de agosto a 7 de septiembre de 1990

misma tecnología nos ha permitido saber de su existencia desde hace sólo unas cuantas décadas atrás.

De esta forma explicaremos la historia de los cinco primeros delitos informáticos de acuerdo a la cronología dada por algunos expertos en la materia. El último delito según la clasificación anterior, se expondrá posteriormente dada su naturaleza y especial desarrollo presentado en la historia de la informática

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

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

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

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

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

En 1987, luego de tratar de poner su vida en orden. cayó ante la tentación y fue acusado, en Santa Cruz California, de invadir el sistema de la compañía Microcorp Systems. Lo sentenciaron a tres años de libertad condicional y luego de la sentencia su expediente desapareció de la computadora de la policía local.

Buscó trabajo en lo que mejor sabía hacer y solicitó empleo en el Security Pacific Bank como encargado de la seguridad de la red del banco. El banco lo rechazó por sus antecedentes penales y Mitnick falsificó un balance general del banco donde se mostraban pérdidas por 400 millones de dólares y trató de enviarlo por la red. Afortunadamente el administrador de la red detuvo el balance antes de que viera la luz.

Ese mismo año inició el escándalo que lo lanzó a la fama. Durante meses observó secretamente el correo electrónico de los miembros del departamento de seguridad de MCI Communications y Digital Equipment Corporation para conocer cómo estaban protegidos las computadoras y el sistema telefónico de ambas compañías

Luego de recoger suficiente información se apoderó de 16 códigos de seguridad de MCI y junto a un amigo, Lenny DiCicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet. Ambos Hackers

querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue un mal cómplice y, a pesar de que habían trabajado juntos, trató de echarle toda la culpa a DiCicco haciendo llamadas anónimas al jefe de éste que trabajaba en una compañía de software como técnico de soporte. Lleno de rabia y frustración DiCicco le confesó todo a su jefe que los denunció a Digital y al FBI.

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

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

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador Gracias a esta maniobra de la defensa Mitnick fue sentenciado a sólo un año de prisión y al salir de ahí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el Hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

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

El fiscal no estaba tan equivocado cuando pidió la restricción del uso del teléfono También en 1992, el Departamento de Vehículos de California ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick por haber tratado de obtener una licencia de conducir de manera fraudulenta, utilizando un código de acceso y enviando sus datos vía fax.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares. De esta manera podría cometer sus fechorías y no estar atado a ningún lugar fijo. Para ello necesitaba obtener programas que le permitieran moverse con la misma facilidad con que lo hacía en la red telefónica

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen Hacker, pero era de los

"chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros Hackers.
Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al Hacker que había invadido su privacidad.

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

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

Al llegar Shimomura a Raleigh recibió una llamada del experto en seguridad de InterNex, otro proveedor de Internet en California. Mitnick había invadido otra vez el sistema de InterNex, había creado una cuenta de nombre Nancy, borrando una con el nombre Bob y había cambiado varias claves de seguridad incluyendo la del experto y la del gerente del sistema que posee los privilegios más altos. De igual manera Shimomura tenía información sobre la invasión de Mitcnick a Netcom, una red de base de datos de noticias.

Shimomura se comunicó con el FBI y éstos enviaron a un grupo de rastreo por radio. El equipo de rastreo poseía un simulador de celda, un equipo normalmente utilizado para probar teléfonos celulares pero modificado para rastrear el teléfono de Mitnick

mientras este está encendido y aunque no esté en uso. Con este aparato el celular se convertiría en un transmisor sin que el usuario lo supiera.
A medianoche terminaron de colocar los equipos en una Van y comenzó la búsqueda de la señal, porque eso era lo que querían localizar: no buscaban a un hombre porque todas las fotos que tenían eran viejas y no estaban seguros de su aspecto actual, el objetivo de esa noche era determinar el lugar de procedencia de la señal Ya para la madrugada localizaron la señal en un grupo de apartamentos pero no pudieron determinar en cuál, debido a interferencias en la señal

Mientras esto ocurría la gente de InterNex, The Well y Netcom estaban preocupados por los movimientos que casi simultáneamente Mitnick hacía en cada uno de estos sistemas Cambiaba claves de acceso que él mismo había creado y que tenían menos de 12 horas de creadas, utilizando códigos extraños e irónicos como no, panix, fukhood y fuckjkt. Estaba creando nuevas cuentas con mayores niveles de seguridad como si sospechara que lo estaban vigilando

El FBI, Shimomura y el equipo de Sprint se habían reunido para planificar la captura. Shimomura envió un mensaje codificado al buscapersonas del encargado en Netcom para advertirle que el arresto se iba a realizar al día siguiente, 16 de Febrero Shimomura envió el mensaje varias veces por equivocación y el encargado interpretó que Mitnick ya había sido arrestado adelantándose a realizar una copia de respaldo de todo el material que Mitnick había almacenado en Netcom como evidencia y borrando las versiones almacenadas por Mitnick. Había que realizar el arresto de inmediato, antes de que Mitnick se diera cuenta de que su información había sido borrada.

Cuando faltaban minutos para dar la orden el simulador de celdas detectó una nueva señal de transmisión de datos vía celular y simultánea a la de Mitnick, muy cerca de esa zona. Algo extraño estaba haciendo Mitnick con las líneas celulares, Shimomura trató de advertirle al agente del FBI pero ya todo estaba en manos de ellos. Shimomura de ahora en adelante no era más que un espectador privilegiado. En el

FBI no pensaban hacer una entrada violenta porque no creían que Mitnick estuviera armado, pero tenían que actuar muy rápido porque sabían el daño que este hombre podía causar en un solo minuto con una computadora. Se acercaron lentamente hasta la entrada del apartamento de Mitnick y anunciaron su presencia, si no les abrían la puerta en cinco segundos la echarían abajo. Mitnick abrió la puerta con toda calma y el FBI procedió a arrestarlo y a decomisar todo el material pertinente discos, computador, teléfonos celulares, manuales, etcétera

De regreso a su hotel Shimomura decide chequear la contestadora telefónica de su residencia en San Diego. Se quedó en una pieza cuando escucho la voz de Mitnick quien le había dejado varios mensajes con acento oriental en tono de burla. El último de estos mensajes lo había recibido ocho horas después de que Mitnick había sido arrestado y antes de que la prensa se hubiera enterado de todo el asunto. Cómo se realizó esa llamada aún es un misterio al igual que el origen y objetivo de la segunda señal de Mitnick.

Este persistente hacker actualmente está siendo juzgado y enfrenta dos cargos federales, uso ilegal de equipos de acceso telefónico y fraude por computadoras. Puede ser condenado por hasta 35 años y a pagar una multa de hasta medio millón de dólares. Mitnick también es sospechoso de robar el software que las compañías telefónicas piensan usar para todo tipo de procesos, desde la facturación hasta el seguimiento del origen de una llamada pasando por la decodificación de las señales de los teléfonos celulares para preservar su privacidad.

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

Kevin Mitnick. Este sencillo nombre, oculta la verdadera identidad de uno de los mayores hackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles y llegó a falsificar 20,000 números de tarjetas de crédito.

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

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

Lunes, 22 de marzo de 1999. REDACCIÓN

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

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

La popularidad de Mitnick, que tiene su pagina en http://www.kevinmitnick.com/home.html, estalló ya en los años 80, cuando fue detenido cuatro veces. Estando en libertad provisional, en 1992, realizó diversas acciones de "hacking", y permaneció como fugitivo hasta su captura, en Carolina del Norte, en 1995.

A partir de ese momento, un buen número de hackers de todo el mundo, deseosos de que se produjera la excarcelación de su mentor, llevaron a cabo diversas acciones de intrusión en sistemas informáticos, el más notorio de los cuales fue el

asalto, en septiembre de 1998. de la pagina del "New York Times", que quedó noperativo durante un par de días. Encarcelado por el Gobierno norteamericano sin uicio, Kevin Mitnick había sido considerado por el FBI como el hacker más peligroso y escurridizo del mundo.

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

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap", mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenia acceso a ordenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados" Explico Murphy "El violar accesos nos resultaba muy divertido". La Banda de hackers fue finalmente puesta a disposición de la ley. Con cargos de robo de propiedad. Murphy fue multado por US $1000 y sentenciado a 2 años y medio de prueba.

-En 1982 dos hackers de los Angeles, Ron Austin y Kevin Poulsen. se introdujeron en la red de intercambio de datos Arpa del Pentágono, la precursora de la actual Internet. La primera opción, en el esquema virtual que poseían, era adivinar la palabra clave de acceso al sistema. Lo lograron al cuarto intento, utilizando las letras JCB, las iniciales de la Universidad de California, en Berkeley Estos saqueadores, aumentaron la capacidad del usuario ordinario UCB, diseñando una subrutina para 'captar" los privilegios del superusuario "Jim Miller". Su "ciberpaseo" terminó al ntentar ojear unos ficheros "cebo", preparados para mantener el mayor tiempo posible conectados a los hackers, pero no sin antes sacar algo de provecho: el

manual de Unix, el sistema operativo multitarea, diseñado por los laboratorios Bell (organismo de investigación de la ATT) la mayor compra telefónica de EE.UU.

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

-Un empleado de una importante empresa ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a " personas ficticias " e imputar los pagos correspondientes a sus sueldos a una cuenta personal de dicho empleado.
Esta maniobra hubiera sido descubierta fácilmente por los mecanismo de seguridad del banco (listas de control, sumarios de cuentas, etcétera) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto el autor produjo cambios en el programa de pago de salarios para que los " empleados ficticios " y los pagos realzados no aparecieran en los listados de control.

Una característica general de este tipo de fraudes, es que en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso en los casos de manipulación del programa, la reiteración puede ser automática, realizada por el sistema sin ninguna participación del autor y cada vez que el programa se reactive. De esta forma el autor de dicho fraude al realizar la

manipulación del programa del banco podría irse de vacaciones, ser despedido de la empresa, o incluso morir, y el sistema seguiría imputando el pago de sueldos a los " empleados ficticios " en sus cuenta personal

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

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

- El 2 de mayo de 1987 Wau Holland y Steffen Wernery , dos hackers alemanes lograron entrar al sistema de la NASA.

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

Desde acá tenemos que poder llegar - murmuró Wau-. Hay que averiguar cómo - contestó Steffen- Probemos algunos. Siempre eligen nombres relacionados con la astronomía, ¿No?

Tengo un mapa estelar: usémoslo Con el libro sobre la mesa, teclearon uno a uno y por orden, los nombres de las diferentes constelaciones.

"Acceso Denegado" - leyó Wau -; maldición, tampoco es este quizá nos esté faltando alguna indicación. Calma pensemos. "set" y "host" son imprescindibles... obvio: además, es la fórmula. Probemos de nuevo ¿Cuál sigue? Las constelaciones se terminaron. Podemos intentar con las estrellas. Haber ¿Castor, una de las dos más brillantes de Géminis? Set Host Castor, deletreó Wau mientras tecleaba.

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

El 2 de mayo de 1987, los dos hackers alemanes, de 23 y 20 años respectivamente, ingresaron sin autorización al sistema de la central de investigaciones aeroespaciales más grande del mundo. ¿Por qué lo hicieron?-Preguntó meses después un periodista norteamericano -.

Porque es fascinante. En este mundo se terminaron las aventuras. Ya nadie puede salir a cazar dinosaurios o a buscar oro. La única aventura posible -respondió Steffen, está en la pantalla de un ordenador. Cuando advertimos que los técnicos nos habían detectado, les enviamos un telex: "Tememos haber entrado en el peligroso campo del espionaje industrial, el crimen económico, el conflicto este-oeste y la seguridad de los organismos de alta tecnología. Por eso avisamos. y paramos el juego". El juego puede costar muchas vidas... ¡Ni media vida! La red en que entramos no guarda información ultrasecreta; en este momento tiene 1,600 suscriptores y 4,000 clientes flotantes.

Con esos datos, Steffen anulaba la intención de presentarlos como sujetos peligrosos para el resto de la humanidad.

-En noviembre de 1988, Robert Morris lanzo un programa "gusano" diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este

programa causó el consumo de los recursos de muchisimas computadoras y que más de 6,000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causó a las víctimas muchos días de productividad perdidos, y millones de dólares. Se creo el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso La sentencia fue criticada fuertemente debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.

-En 1988, varios hackers consiguieron entrar en los ordenadores de siete universidades de Gran Bretaña, la de Londres incluida. Para resolver este crimen, la policía necesitó la ayuda técnica de un asesor informático, Robert Jones Una vez arrestado el sospechoso, las pruebas se analizaron durante un año y medio antes de presentarlas ante el tribunal, que lo condenó a un año de prisión. Después de varias colaboraciones más, Scotland Yard propuso la creación de un centro universitario dedicado a la investigación de estos casos. El Centro de Investigación de Delitos Informáticos, adscrito al Queen Mary & Westfield College, se creó a principios de 1996 y el abogado Ian Walden, experto en la legislación de tecnología de la información, es su director. El Centro obtiene fondos del Gobierno y se dedica a la investigación y la asesoría en el campo de los delitos informáticos, así como a impartir cursos de formación en la materia para policías, fiscales, abogados y cualquier interesado.
En 1989 la justicia alemana detiene a un grupo de crackers germanos que habían copiado durante años miles de programas de acceso no legal y passwords de ordenadores en departamentos de la administración de EEUU. El destinatario de la información era el KGB soviético.

-Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de "Dark Dante" en las redes de computadoras es acusado de robar órdenes de tarea

relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.
Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel 5 años, fue liberado en 1996, supuestamente "reformado". Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker

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

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

-Todos estos asaltos no suelen tener consecuencias importantes, pero lo peor de todo es cuando lo efectúan los "chicos malos" (crackers o hackers de contraseñas). Uno de los casos más destacados es el que se produjo en 1994, cuando varios "piratas" consiguieron introducirse en el sistema de seguridad de la Florida State University, violándolo y llevándose consigo varias copias de prueba de Windows 95, uno de los más potentes sistemas operativos de Microsoft, que en aquel entonces no era comercial ni público.
En 1994 crackers americanos se hacen vía Internet desde Mallorca con 140,000 números de tarjetas de crédito telefónicas de EEUU. Usuarios de todo el mundo llaman a cuenta de las víctimas. El fraude llega a los 140 millones de dólares perdidos por compañías como Bell Atlantic, MCI o AT&T.

-En 1994 David La Macchia, estudiante de 20 años del prestigioso y serio MIT, reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por un valor de 1 millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS. Todo un escándalo que manchó el nombre de esta mítica institución universitaria.

-Levin, Vladimir, un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street. Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia. Alemania, Israel, Holanda y Suiza fondos por un valor de 10 millones de dólares según el FBI. Detenido en el Reino Unido a principios de 1995. Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.

-En el año de 1974 un 28 de marzo, nació en Río Gallegos Julio Cesar Ardita, considerado el hacker más famoso de Argentina. En la primaria tuvo el honor de ser abanderado. Curso la secundaria en un pequeño colegio del barrio porteño de Caballito, el Dámaso Centeno, en donde por primera vez utilizo una computadora. En quinto año, junto con dos compañeros ayudaron a informatizar el sistema de notas y facturación del colegio en el cual estudiaba.

Julio César Ardita - el pirata informático más famoso de la Argentina- en su declaración por la causa penal por estafa que se le inició en Argentina. Hijo de Julio Rafael Ardita, un teniente coronel retirado del Ejercito Argentino, y de la docente Susana Colombo, el joven creció viajando por todo el país hasta terminar, a los 14 años, en la Capital Federal. Por supuesto, todavía no conocía de computadoras conectadas con teléfonos y mucho menos, de abogados, jueces y periodistas que lo buscaran sin suerte para que contara su ¡travesura!. Como Ardita, son miles los jóvenes de la aldea global que se dedican a violar códigos secretos, vulnerar accesos restringidos y burlar herméticos vallados en redes telemáticas por el simple desafío de derribar murallas de seguridad informática

También conocidos como hackers en la jerga cibernética, estos sujetos de apodos extraños, suelen militar en las filas del anonimato y el bajo perfil hasta que su

actividad es descubierta y estallan los escándalos. Si, tal cual sucedió en el caso Ardita.

Este muchacho, que hoy tiene 24 años y administra una exitosa empresa de seguridad informática, saltó a la fama el 28 de diciembre de 1995, día de los Santos Inocentes, cuando su domicilio fue allanado por la Justicia Argentina luego de que los Estados Unidos alertaran sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Las intrusiones provenían de una computadora conectada a una línea telefónica desde un departamento del Barrio Norte, en la Capital Federal. Y eran obra del mayor de cuatro hermanos, un incurable noctámbulo de 21 años, apasionado por la telemática, que utilizaba el seudónimo de "el Gritón" y se colaba en la red de computadoras de la empresa Telecom a través de líneas telefónicas 0800 de uso gratuito para consumar sus intromisiones en sistemas informáticos ajenos

En la Argentina, "el Gritón" todavía no saldaba sus cuentas con la Justicia. la juez Wilma López, a cargo del Juzgado de Instrucción 38, dispuso que Ardita compareciera ante un tribunal oral pero por fraude telefónico (¡¡estimado por la empresa Telecom en 50 pesos!!), ya que las intrusiones informáticas no están contempladas en el Código Penal. El juicio se concretaría antes de fin de año y sería el primero de estas características que se realice en Argentina. Sin embargo, por el mismo episodio, Ardita ya tuvo que recorrer una espinosa demanda penal en los Estados Unidos, donde las intrusiones informáticas, las violaciones de códigos secretos y la posesión de claves ajenas sí son delitos graves. El proceso terminó el 19 de mayo pasado, cuando un tribunal de la ciudad de Boston, sobre la costa noreste estadounidense, lo condenó a 3 años de libertad condicional y a pagar una multa de 5000 dólares por haber vulnerado, entre otros, el sistema informático de la Marina. Desde entonces, el hermetismo que rodeó al proceso judicial que se le abrió en la Argentina alimentó el interés acerca del pirata informático que, con una simple computadora instalada en su cuarto, puso en estado de alerta a los servicios de inteligencia de los EE.UU, al FBI y al propio Departamento de Justicia estadounidense.

Parte de ese misterio (Ardita jamás dio una entrevista y ningún medio logró fotografiarlo) puede ser develado a través de su propia declaración en la causa número 45048/95, con carátula "Ardita Julio C., sobre defraudación", realizada en abril de 1996 en el juzgado de Instrucción número 38. Martín Niklison, fiscal de la causa, recuerda perfectamente al más famoso hacker criollo Dice que Ardita "es una persona muy arrogante, de una pedantería tal que simplificó la acusación. Su soberbia lo llevó a reconocer todos y cada uno de los hechos que se le imputaban". ¿Por que no habría de hacerlo? Si, después de todo, la jurisprudencia argentina no contempla los llamados "delitos informáticos". No hay ley en el Código Penal que tipifique, por ejemplo, la intrusión en computadoras ajenas.

Además de la actividad informática en el colegio Dámaso Centeno, Ardita aprendió por su cuenta compró algunas computadoras muy rudimentarias hasta llegar a la PC. Luego inició la carrera de Ciencias de la Computación en la Universidad de Buenos Aires y "por interés vocacional compraba libros de computación, programación y, sobre todo, de seguridad informática", según puntualizó en el juzgado En febrero del 95, Julio Ardita viajó a la ciudad de Chicago, Estados Unidos. "Allá fue donde inició sus investigaciones relacionadas con Internet Todo comenzó cuando vió que tenían computadoras conectadas a la gran red y eso le llamó mucho la atención ¨ Era importante hace algunos años el uso de la Internet, que hoy es de lo mas común, todavía era un privilegio para muy pocos ¨ Por eso, detallar en un juzgado que era la red, como consiguió concretar a través de ésta comunicaciones internacionales desde su casa sin abonar un solo peso, fue una dura tarea para el hacker Ante el desconcierto de la juez, el fiscal y los abogados, Ardita necesitó gráficos para explicar como ingresó a la red interna de computadoras Telconet (de Telecom) a través de una línea 0800. ¨ Lo que hice -dijo- fue llamar utilizando mi PC a todos los números de una central telefónica ¨. Para eso usó un programa pirata llamado Toneloc. Y así, según declaró, averiguó el número telefónico para acceder a la Telconet. Sin embargo, para ingresar a la red interna de la empresa Telecom es necesario poseer una clave secreta de 14 dígitos. Cada usuario legítimo tiene una. Por eso, en un principio, la investigación apuntó a que algún contacto dentro de la

empresa telefónica le hubiera facilitado el código. Pero Ardita demostró que, para él, la cuestión había sido mucho más simple: "Cuando uno establece la conexión con la Te lc on et y presiona simultáneamente las teclas 'Ctrl-p' y luego tipea 'STAT', el sistema da mucha información", confesó. La denominación 'STAT' es tomada por el sistema informático como "status" y pone en pantalla la información de los últimos accesos de personal validado por el sistema, con sus nombres de usuarios y sus claves secretas de 14 dígitos. Los asistentes, que escuchaban con atención y bastante incredulidad, a duras penas podían seguir ese vocabulario inédito y estrafalario que empleaba "el Gritón"

Según siguió su declaración, cuando sorteó la primera valla de seguridad informática encontró un bocado de lo más apetecible: la red de computadoras que Telecom tenía conectada a Internet. Sólo que, para ingresar, era necesario ser usuario legal "Comencé entonces a probar con distintos nombres de personas: María, Julio, etcétera, pero con el nombre Carlos obtuve respuesta", aseguró Ardita al Tribunal. Así, a través del sistema de prueba y error, llegó a navegar por Internet enganchado a la sede comercial Clínicas (de Telecom) sin desembolsar un peso por acceso a la red ni por pulsos de teléfono. Ese fue el golpe inicial de sus problemas judiciales, ya que, desde allí ingresó al sistema de la Universidad de Harvard que, a su vez, le sirvió de trampolín para acceder a los de la Marina de los EE.UU. y del Laboratorio de Propulsión Nuclear de la NASA, entre otros tantos. "El objeto de todas mis incursiones en Internet fue la investigación", se disculpó Cuando ingresó al sistema de la Marina estadounidense fue detectado y rastreado por el FBI y el Servicio de Investigaciones Criminales de la Marina de los EE.UU.

En el juicio de Boston (realizado allí porque es donde está la Universidad de Harvard), lo condenaron puntualmente por posesión fraudulenta de claves de seguridad, nombres de abonados legítimos, códigos y otros permisos de acceso; por actividad fraudulenta y destructiva con computadoras y por interceptación ilegal de comunicaciones. Hoy en día, con 24 años, Julio Cesar Ardita paga religiosamente sus facturas telefónicas. Además, se levanta temprano por las mañanas y camina

hasta la zona de Tribunales. Allí está Cybsec S.A., la exitosa empresa de seguridad informática que ahora el ex ciberpirata administra junto a su socio. Sus embrollos judiciales le permitieron entablar múltiples contactos en la Argentina y en el exterior. "La metamorfosis de hacker romántico a yuppie experto en seguridad informática suele ser habitual", sostienen los conocedores del rubro. En tanto, en Buenos Aires, su caso despertó mucha expectativa: juristas y entendidos en computación estarán pendientes de la resolución de su juicio. Seguramente, "el Gritón" hablará en un tono más bajo, sin anonimato ni demasiadas huellas de aquellos tiempos de rebeldía juvenil, cuando enfrentaba, de puro apasionado, los desafíos de la Informática.

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

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de 10,000 dólares. Melissa en su "corta vida" había conseguido contaminar a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

En España su "éxito" fue menor al desarrollarse una extensa campaña de información, que alcanzó incluso a las cadenas televisivas, alertando a los usuarios de la existencia de este virus. La detención de David Smith fue fruto de la colaboración entre los especialistas del FBI y de los técnicos del primer proveedor de servicios de conexión a Internet de los Estados Unidos, América On Line. Los ingenieros de América On Line colaboraron activamente en la investigación al descubrir que para propagar el virus, Smith había utilizado la identidad de un usuario de su servicio de acceso. Además, como a otros proveedores el impacto de Melissa

había afectado de forma sustancial a buzones de una gran parte de sus catorce millones de usuarios.

Fue precisamente el modo de actuar de Melissa, que remite a los primeros cincuenta inscritos en la agenda de direcciones del cliente de correo electrónico "Outlook Express", centenares de documentos "Office" la clave para encontrar al autor del virus. Los ingenieros rastrearon los primeros documentos que fueron emitidos por el creador del virus, buscando encontrar los signos de identidad que incorporan todos los documentos del programa informático de Microsoft "Office", y que en más de una ocasión han despertado la alarma de organizaciones en defensa de la privacidad de los usuarios. Una vez desmontado el puzzle de los documentos y encontradas las claves se consiguió localizar al creador de Melissa. Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar. Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

-En agosto de 1995, Adam Back (británico), Eric Young (australiano) y David Byers (sueco), demuestran en Internet como pueden violarse en cuestión de minutos los algoritmos de seguridad de Netscape Navigator, el programa de acceso a WWW más usado mundialmente. Al mes siguiente, los cyberpunks americanos David Wagner y Ian Goldberg crean un método para violarlo en sólo 25 segundos.

-En 1996 Public Access Networks Corp., una de las grandes empresas dedicadas al suministro de acceso a la red de Estados Unidos, que controla las páginas de más de 1,000 empresas en la World Wide Web, sufrió un feroz ataque por parte de piratas informáticos. Estos llevaron a la locura a los ordenadores de la empresa mediante el continuo envío de solicitudes de información adulteradas, más de 150 por segundo. Como ejemplo, tenemos lo que sucedió el 19 de Septiembre de 1996, cuando la CIA sufrió los ataques de un grupo de Hackers suecos, que desmantelaron su servidor de

Información en Internet, modificando el mensaje de presentación "Bienvenidos a la Agencia Central de Inteligencia" por "Bienvenidos a la Agencia Central de Estupidez" Entre la maraña de contenidos de la Web, colocaron también varias conexiones directas a otros lugares de Internet, como a las revistas Flashback o Playboy. La CIA experimentó una grave derrota, con lo que tuvo que retirar su maltrecho servidor.

-En 1996 el Grupo Antipiratería de la empresa de software Novell, informaba de la captura de un individuo que respondía al alias de "El Pirata". Con la colaboración de la Policía de Zurich, Novell consiguió atrapar a este cracker que ofrecía productos de la compañía a usuarios de Internet de forma ilegal con un valor de 60,000 dólares, junto con software comercial de otros miembros de la BSA (Business Software Aliance). Se localizaron también instrucciones para realizar operaciones fraudulentas con tarjetas de crédito. Sus acciones le pueden llevar a ser condenado un máximo de tres años y/o una multa de 10 millones de pesetas por ello. Martin Smith, el Director de Programas de Licencias de Novell para Europa, Oriente Medio y África, lo valora así: "Éste es un caso clave para el futuro de la industria del software. Desde hoy los individuos y organizaciones que distribuyen software ilegal en Internet saben que pueden ser capturados y procesados".

-Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores más utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", ¡accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante: "¡Todos los que el mes pasado utilizaron el motor de búsqueda Yahoo! han adquirido una bomba lógica que se activará el día de Navidad, sembrando el caos en todas las redes informáticas del planeta". Y añadían que solo entregarán el antídoto del virus si Mitnick, condenado a 35 años de prisión, quedaba en libertad. La bomba no pasó de ser una amenaza, pero el efecto de llamar la atención sobre el caso Mitnick se había conseguido.
Si cumplían con sus requisitos, el programa antídoto, oculto en un ordenador, sería suministrado a los cibernautas. Todo se quedó en palabras, porque según la portavoz de Yahoo, Diane Hunt, los hackers accedieron a la página de la empresa,

pero no destruyeron ni infectaron nada. Todo fue una falsa alarma... pero ¿y sí hubiera sido cierto?.

-En Mayo de 1997, un grupo de hackers ("cortadores") asalta la página de una de las películas más taquilleras de la fábrica Spilberg: Jurassic Park, cambiando durante 18 horas el logotipo del dinosaurio por otro en el que aparecía un pato. Los servicios de inteligencia están protegidos por poderosas "articulaciones" de los estados, y gozan de una fama y de un prestigio internacionales, pero los hackers logran con su espontaneidad bajarle los humos al brazo armado del poder, y perpetuar el carácter secreto y anárquico de sus organizaciones, consiguiendo de paso, unos buenos "titulares".

Nadie está fuera del alcance de estos saqueadores, ni siquiera el todopoderoso Bill Gates, que vio como la Homepage de Microsoft fue atacada por varios hackers en junio de 1997. Estos hackers, accedieron al sistema operativo por un bug de Windows Nt 4 0, el cual era el servidor bajo el que se ejecutaba la Web de Microsoft. Hay muchas formas de dar publicidad a actos "presumiblemente ilegales", pero algunas son más ingeniosas que otras.

Algunos hackers consiguen que sus hazañas sean universalmente conocidas, dejándose "atrapar" por la justicia, o incluso en ocasiones, llegando a negociar las penas de cárcel por escuchas y accesos ilegales. Este es el caso de J.C Ardita, un hacker argentino (antes mencionado) que en Diciembre de 1997 se confesaba culpable de los cargos que se le imputaban, y volvía voluntariamente a Estados Unidos para que se le juzgara por los delitos cometidos.

-Una de las hazañas más sorprendentes de intercambio de información entre hackers fue el caso Price. En esta ocasión, se investigó la acción de un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde allí conseguía entrar en los ordenadores del Ministerio de Defensa de los Estados Unidos. Llegó a copiar archivos que no eran materia reservada, pero sí investigaciones de temas delicados Su centro de trabajo era su casa, en Londres, y desde allí causó uno de los mayores

desastres informáticos de la década. No trabajaba solo, por que intercambió todos los documentos que había obtenido con hackers de distintos países, vía Internet. El caos fue total, llegando incluso al cierre temporal de la red norteamericana. Estos grupos tienen una forma de operar muy estricta, y la exclusión de uno de sus miembros significa la recesión total de privilegios, y la condena al destierro virtual. Fidelidad, confidencialidad y tenacidad son los rasgos más comunes entre los hackers.

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

-En 1997 se publica el libro "Takedown" de Tsutomu Shimomura y John Markoff de la editorial El País-Aguilar de 464 páginas, en el se relatan la busqueda y captura de un escurridizo hacker que domina el arte del "IP-spoofing", que consiste en producir falsos números IP para ser reconocido por otras máquinas conectadas y pasearse por su interior. Es un reportaje novelado, contado en primera persona por el experto en seguridad Tsutomu Shimomura, que fue saqueado por el hacker en plena navidad del 94 y dedicó medio año a detenerle. Lo escribió junto a John Markoff, un periodista del New York Times que había seguido el caso.

Microsoft ha anunciado firmes avances en su lucha contra el delito informático durante el año fiscal de 1997, que incluye el embargo de cerca de 100,000 copias ilegales o programas falsos, CD-ROM y dispositivos hardware, procedentes de canales de distribución europeos y con un valor de más de 23 millones de dólares

-Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 1998, a la tierna edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa. Simplemente fueron formados por algún "experto hacker", que se encontraba a miles

de kilómetros de su pueblo natal, Cloverdale, y que se hacía llamar el "Pirata Maestro"

Estas acciones no son novedosas en el mundo del Hacking. El mayor sueño de un recién estrenado hacker es "colarse" en las profundidades del mayor organismo de seguridad del mundo, pero normalmente el riesgo que entraña, y sus consecuencias legales, hace que se decanten por ordenadores de Universidades, o de empresas que no son muy conocidas.

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

" MANIFIESTO HACKER.
Uno más ha sido capturado hoy, está en todos los periódicos. Joven arrestado en escándalo de Crimen por Computadora , Hacker arrestado luego de traspasar las barreras de seguridad de un banco Malditos muchachos todos son iguales. Pero tú, en tu psicología de tres partes y tu tecnocerebro de 1950, ¿haz alguna vez observado detrás de los ojos de un Hacker? ¿Alguna vez te haz preguntado qué lo mueve, qué fuerzas lo han formado, cuáles lo pudieron haber moldeado? Soy un Hacker, entra a mi mundo. El mío es un mundo que comienza en la escuela. Soy más inteligente que la mayoría de los otros muchachos, esa basura que ellos nos enseñan me aburre. Malditos subrealizados son todos iguales. Estoy en la preparatoria, he escuchado a los profesores explicar por decimoquinta vez como reducir una fracción Yo lo entiendo No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente.
Maldito muchacho. Probablemente lo copió, todos son iguales. Hoy hice un descubrimiento. Encontré una computadora. Espera un momento, esto es lo máximo

Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué. No porque no le gustó, o se sienta amenazada por mi, o piense que soy un engreído, o no le gusta enseñar y no debería estar aquí.

Maldito muchacho, todo lo que hace es jugar. Todos son iguales. Y entonces ocurrió, una puerta abierta al mundo corriendo a través de las líneas telefónicas como la heroína a través de las venas de un adicto, se envía un pulso electrónico, un refugio para las incompetencias del día a día es buscado Una tabla de salvación es encontrada. `Este es... este es el lugar a donde pertenezco. ´ Los conozco a todos aquí... aunque nunca los hubiera conocido, o hablado con ellos, o nunca vuelva a escuchar de ellos otra vez. Los conozco a todos.

Malditos muchachos Enlazando las líneas telefónicas otra vez. Todos son iguales.. .Apuesta lo que sea a que todos somos iguales . . .A nosotros nos han estado dando comida para bebés con cuchara en la escuela, cuando estábamos hambrientos de carne Las migajas de carne que ustedes dejaron escapar estaban masticadas y sin sabor. Nosotros hemos sido dominados por sádicos, o ignorados por los apáticos. Los pocos que tienen algo que enseñarnos encontraron alumnos complacientes, pero esos pocos son como gotas de agua en el desierto. Ahora este es nuestro mundo...

El mundo del electrón y el conmutador, la belleza del baudio. Nosotros hacemos uso de un servicio que ya existe sin pagar por lo que podría ser barato como el polvo, si no estuviera en manos de glotones hambrientos de ganancias, y ustedes nos llaman criminales. Nosotros explorámos y ustedes nos llaman criminales. Nosotros buscamos detrás del conocimiento... y ustedes nos llaman criminales. Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos y ustedes nos llaman criminales. Ustedes construyeron bombas atómicas, ustedes hicieron la guerra, ustedes asesinaron, engañaron y nos mintieron y trataron de hacernos creer que era por nuestro bien, ahora nosotros somos los criminales. Si, soy un criminal. Mi crimen es la curiosidad. Mi crimen es el juzgar a las personas por lo que dicen y piensan, no por lo que aparentan. Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás. Soy un Hacker, este es mi manifiesto. Tu podrás detener este esfuerzo

individual, pero nunca podrás detenernos a todos.. después de todo, todos somos iguales.

+++The Mentor+++ [2]

HISTORIA DE LOS VIRUS (TIPO DEL DELITO INFORMÁTICO).

Como se señalo en el principio de este punto 1.2, la historia del virus vale la pena explicarla de manera separada debido a su especial desarrollo, ya que maneja distintas formas de presentarse, así como diferentes lugares en el mundo.

Información fidedigna que pueda confirmar el nacimiento de los virus y los contagios virales, que exista, es realmente dudosa, debido a que los grandes organismos gubernamentales, científicos o militares ocultaron la verdad respecto a los virus cuando llegaron aparecer infecciones en sus sistemas.

Esto se debe a que ninguno de ellos acepta reconocer que sus equipos y programas podían ser vulnerables frente a los virus, ya que estos sistemas de seguridad que se suponían que nadie ajeno al sistema podría burlar

Solamente una serie de hechos y nombres aislados se han difundido en los medios especializados, como revistas científicas y de computación y dan una pobre visión del proceso de desarrollo de los Virus Informáticos, pero más adelante se tratara de dar una clara idea de su historia. Sin duda alguna la historia de los virus informáticos es un complemento de cómo fue el desarrollo de los delitos informáticos, ya que no podemos hablar de los delitos informáticos sin mencionar el origen y la evolución de los virus informáticos.

Nuemann, John Von (1903-1957), matemático estadounidense nacido en Hungría. que desarrolló la rama de las matemáticas conocida como teoría de juegos. Nació en Budapest y estudió en Zurich y en las universidades de Berlín y Budapest Viajó a Estados Unidos en 1930 para unirse al claustro de la Universidad de Princeton. En 1949 en el Instituto de Estudios Avanzados de Princeton, Nueva Jersey, planteó la posibilidad teórica de que un programa informático se produjera a través de su libro

[2] Pagina Internet http //renel cbj net, VII Hackers

titulado ' Theory and Organización of complicated Automata ' (Teoría y Organización de Autómatas Complejos) .

Esta teoría se comprobó experimentalmente en la década de 1950 en los laboratorios de computación de AT & T (Bell laboratorios), donde varios científicos norteamericanos, H.Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson, este último ingeniero en sistemas creador de la primera versión del sistema Unix, para entretenerse inventaron un juego al que llamaron Core Wars. inspirados en un programa escrito en lenguaje ensamblador llamado Creeper. el cual tenia la capacidad de reproducirse cada vez que se ejecutaba. El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la memoria del rival o impedir su normal funcionamiento

También diseñaron otro programa llamado Reeper el que sería el antivirus en ese momento, cuya función era diseñar el destruir cada copia hecha por Creeper. Estaban conscientes de la peligrosidad que representaba para los sistemas de computación y prometieron mantenerlo en secreto, pues sabían que en manos irresponsables el Core War podría ser empleado nocivamente.
En el año de 1974, la Xeros Corporación presentó en Estados Unidos el primer programa que ya contenía un solo código autoduplicador.
Los equipos Apple II se vieron afectados a fines de 1981 por un virus llamado Cloner que presentaba un pequeño mensaje en forma de poema. Se introducía en los comandos de control e infectaba los discos cuando se hacia un acceso a la información, utilizando el comando infectado.

En 1983. el ingeniero eléctrico estadounidense Frederick B.Cohen, que en ese entonces era estudiante en la Universidad de California, expuso por primera vez por escrito el concepto actual de " virus informático ", durante el desarrollo de una conferencia sobre seguridad. Se trataba de la National Computer Security Conference. celebrada en Toronto, Canadá. Donde describió un programa

informático que se reproduce así mismo, es decir el primer virus residente en una PC, por lo que hoy se le conoce como el " Padre de los Virus Informáticos ".

Los denominó también "Trojan Horses" y "Worms" (caballos de troya y gusanos). Apareciendo en 1985 los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sin número de virus cada vez más complejos.
El primer contagio masivo de microordenadores se dio en 1987 a través del MacMag (virus llamado también Peace Virus) sobre ordenadores Macintosh. Dos programadores (uno de Montereal, Richard Brandow y el otro de Tucson, Drew Davison), crearon un virus y lo incluyeron en un disco de juegos que repartieron en una reunión de un club de usuarios. Uno de los asistentes Marc Canter, consultor de Aldas Corporation, se llevó el disco a Chicago y contaminó su ordenador. Al realizar pruebas al paquete Aldus Freehand contaminó el disco maestro que posteriormente devolvió a la empresa fabricante. Allí la epidemia se extendió y el programa se comercializó con el virus incluido. El virus era bastante benigno y el 2 de Marzo de 1988 (primer aniversario de la aparición del Macintosh II) hizo público en la pantalla un mensaje pidiendo la paz entre los pueblos y se destruyo así mismo. Se estima que este virus afecto a doscientos cincuenta mil ordenadores en todo el mundo.

Existe una versión de este virus detectada en la red internacional de correo electrónico de IBM y al que se denomina IMB Christmas Card o Xmas que felicita el 25 de diciembre. Se calcula que afecto a trescientos mil terminales en todo el mundo En Diciembre de 1987, los expertos de IBM tuvieron que diseñar un programa antivirus para desinfectar su sistema de correo interno, pues éste fue contagiado por un virus dañino que hacia parecer en las pantalla de las computadoras conectadas a su red un mensaje navideño, el cuál al reproducirse así mismo, múltiples veces, hizo muy lento el sistema de mensajes de la compañía, hasta el punto de paralizarlo por sesenta y dos horas.

El virus presentaba un mensaje navideño con un árbol al lado y pedía al usuario que tecleara la palabra "Christmas" Si tecleaba la palabra , el virus se introducía en la lista de correspondencia del correo electrónico del operador y seguía diseminándose por toda la red. De no acceder a la demanda y apagar el equipo, el virus impedía que se pudiera grabar los trabajos inconclusos, perdiéndose horas de trabajo.

El primer virus de contagio realmente masivo en el mundo de los ordenadores compatibles, funcionando bajo sistema operativo MS-DOS, es el "Pakistani Brain" , que fue detectado por primera vez en la Universidad de Delaware, en Estados Unidos, en el mes de Octubre de 1987. Este virus, al parecer escrito y difundido por dos hermanos de Pakistán, estudiantes de la Universidad de Lahore, es del tipo "Boot" , es decir es de los que desplazan el sector de arranque y se alojan en él, tomando el control del ordenador, incluso antes que el sistema operativo lo haga.

En Lahore, Pakistan, existía una tienda de informática especializada en la venta pública de software comercial pirateado. Los turistas de países más industrializados se encontraban con la sorpresa de poder comprar las últimas versiones de los programas más difundidos a muy bajo precio. Pero algún problema debió existir entre éstos hermanos (Amjad Farooq Alvi Y Basit Farooq Alvi) y el dueño de la tienda, a los que al parecer los unía alguna relación comercial. Estos diseñaron el virus e infectaron los disquetes que se distribuían en la tienda.

La infección afecto principalmente a Estados Unidos y Canadá, al parecer los turistas provenientes de estos países eran los mejores clientes de la tienda. Al estar los programas desprotegidos, su difusión fue más ágil. El virus es notoriamente descarado para los tiempos que corren, la etiqueta de volumen cambia a "(C) Brain ", con lo que con un simple DIR se detecta. En el sector de arranque incluye gran cantidad de texto y a continuación se transcribe una pequeña parte de éste:
"Brain Computer Services 730 Nizam Blokc Allamaiqbal Town.
Lahore-Pakistan

Phone: 430791, 443248, 280530"

Este virus esta ahora casi desaparecido, pero existen mutaciones suyas que tienen aún hoy gran difusión Actualmente está muy activa la que incluye el texto "Virus Shoe Record v9 0" y también v9.1. Estos mensajes permanecen en el sector de arranque y nunca se ven por pantalla.

El descaro de estos virus no es inusual, un ejemplo es el del virus Sylvia o Holland Girl. Al parecer escrito por el ex novio de una chica holandesa, en el código del virus se encuentra el teléfono y la dirección postal de la chica, solicitando que se le llame o se le envíen postales, (suponiendo que para pedirle que no abandone a su novio)

El 13 de Mayo de 1988, fue detectado un virus por primera vez en la Universidad Hebrea de Jerusalem. El virus llamado "Viernes 13", casualmente en el cuarenta aniversario de la fundación del Estado Judío El virus se difundió por la red de la Universidad e infecto ordenadores del ejército israelí, el ministerio de educación. etcétera. Este mismo virus fue difundido en España por el disco de la revista "Tu ordenador Amstrad"(en mayo de 1989). La gran difusión publicitaria de este virus a través de los medios de comunicación, ha provocado que este sea uno de los virus con más número de mutantes (al menos dos de ellos se han fabricado en España posiblemente en Barcelona).

Este es un virus de posible intencionalidad política, de hecho uno de sus nombres es PLO (Organización de Liberación Palestina), y tampoco es el último. El virus Fu Manchú intercepta el buffer del teclado y detecta el nombre de varios políticos (Reagan, Thatcher, Botha, Waldheim), vertiendo insultos (y otros dicen que los interpretan como divertidos comentarios), sobre ellos cada vez que su nombre se teclea. Los mensajes que aparecen, después de teclear nombres son los siguientes:
Reagan is an arsehole, Thatcher is a cunt, Botha is bastard, Waldheim is a nazi.

Últimamente ha aparecido el virus Kennedy de origen americano, al parecer dedicado a la conocida saga familiar de políticos norteamericanos, aunque tampoco se descarta la vinculación de este nombre con el desaparecido grupo musical Dead Kennedy´s que también mostró en numerosas ocasiones su desprecio por la familia Kennedy.
Muy difundido fue el caso Robert Morris en noviembre de 1988, que contaminó toda la red de Internet y sus asociadas incluyendo a la red del Pentágono, Arpanet, paralizando gran número de ordenadores estatales. Los daños causados se calculan en unos 100 millones de dólares y por lo que en el año de 1989, se llevo a tribunales de Estados Unidos el caso de Robert Morris (hijo), de tal manera que actualmente se encuentra procesado.

Recordando el programa Core War, desarrollado desde hace más de 20 años por científicos de los laboratorios Bell, de los cuales era Robert Morris, se sabe que su hijo, trabajo ahí en unas vacaciones de verano. Conoció el programa y lo divulgo entre algunos amigos, los cuales se encargaron de diseminarlo.

En Octubre de 1989 lo virus eran considerados una terrible epidemia. Hechos deplorables comenzaron a suceder. Un comunicado tecnoterrorista manifestaba que había infectado una gran cantidad de computadoras, y que el viernes 13 se destruiría automáticamente los archivos almacenados en disquetes o en discos fijos, desatando el pánico entre los usuarios, fundado básicamente en la superstición que provoca esa fecha.

Aunque no se realizó esa catastrófica profecía, sirvió para replantar el grave peligro al que están dispuestos los datos de cualquier sistema. En Estados Unidos sesenta computadoras de la NASA fueron infectadas y el programa intruso se siguió reproduciendo por medio de la red comercial que tiene con empresas privadas de su país Se calcula que más de medio millón de PCs y muchos de los Bancos de datos Internacionales han sido atacados por diversos tipos de virus.

Se considera que son más de dos mil virus de los que se conocen en la actualidad, incluyendo sus variantes los existentes hoy en día.
Los virus de hoy , no solamente copian sus códigos en forma parcial a otros programas, sino que además lo hacen en áreas importantes de un sistema (sector de arranque, Fat´s, Tabla de particiones, etcétera). En segundo lugar un virus no tiene necesariamente que auto reproducirse pues basta que se instale en memoria y de ahí lance un artero ataque a un determinado tipo de archivos o áreas del sistema y los afecte. Es decir, que el virus ya no requiere hacer copias de si mismo.

Existen virus de reciente generación denominados 'Bombers' que al ser ejecutados una sola vez logran inmediatamente el MBR (Master Boot Root) y es prácticamente imposible continuar operando el sistema con el cuál su detección es muy difícil pues su micro código es auto destruido. Esos tipos de virus usan técnicas denominada Infectar Rápido.

Un ejemplo de las distintas actividades terroristas de algunos grupos en varios países que se han realizado a lo largo de estas últimas dos décadas son las siguientes:

En Estados Unidos un grupo tecnoterrorista se hace llamar La Plaga y en sus mensajes incluye slogans como " Quisiera ver más virus por ahí " y amenazan con infectar sistemas de todo el mundo, incluyendo China y Rusia, en donde ya existe un virus llamado " Lágrimas que caen como cascada " y hace que las letras que se están viendo en la pantalla caigan como una lluvia y se amontonen en la parte inferior de ésta.

Otros virus presentan en la pantalla a la cantante norteamericana Madonna bailando al ritmo de una pieza musical, y mientras el usuario observa con asombro aquel ritual, sus archivos son borrados al mismo ritmo. Existe un virus gastronómico, el cual contagio la computadora DECsystem 10. La característica de este pequeño

personaje era que permanecía latente por tiempo indefinido en el sistema y cuando se activa presenta en la pantalla el mensaje "I want a cookie".

El virus que actúa de tal manera que cuando detecta cantidades de cuatro cifras, las reacomoda alterando el orden, lo que hace que cuando el operario trabaja con números (estados de cuenta, cobranzas, etcétera) utilice cantidades falseadas.

El colmo del terrorismo víral ha sido que hasta los mismo programas " vacunas ", que se supone que deberían ser los más confiables, han sido modificados por los Ciberpunks. De esta manera el magnífico programa FluShot, que se difundió por medio de los Bullettin Board Systems o sistemas de software compartido (Shareware), infecto los programas de cientos de usuarios que venían en el programa de bajo costo y con muy buenas perspectivas en la lucha contra los virus.

Todo esto ha llevado a personas como Ross M. Greenberg, (creador del mencionado programa Flushot), y a víctimas de esas infecciones vírales en sus programas, a ofrecer una recompensa a quien proporcione informes y denuncie a los Ciberpunks de La Plaga.

En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept

En la actualidad, la sociedad empieza a reaccionar para defenderse de este fenómeno; las leyes comienzan a cambiar para adecuarse a este nuevo tipo de delito informático, si bien las empresas son reacias a confesar que sufren las consecuencias de los virus por temor a perder prestigio.

En Estados Unidos ya funciona la Computer Virus Industry Association que contabilizó el año 1988 más de noventa mil casos de ordenadores infectados en empresas, y en 1989 por encima del medio millón, por lo que su cifra bien podría ser

el doble en la realidad. Ello indica que el fenómeno se extiende en proporción geométrica. Si bien las cifras citadas se refieren a todo tipo de ordenadores, debemos considerar que se estima que el parque actual de compatibles IBM-PC en el mundo supera los 37 millones En España, este papel lo ha tomado la Asociación Española de Empresas de Software (A-Soft), si bien su papel prácticamente se redujo a un somero seguimiento del brote epidémico del Viernes 13, y a la distribución gratuita de programas específicos contra ese virus y el troyano AIDS

La industria informática no para de generar programas, e incluso hardware, para luchar contra los virus informáticos, creando una nueva especialidad dentro de la informática de gestión.

Actualmente los virus pueden recorrer miles de kilómetros en pocos minutos. La moda americana de los BBS (Bulletin Board System), especie de club de usuarios al que se accede vía modem telefónico, ya está llegando al resto de los países Las redes nacionales e internacionales (como FIDONET) abundan y aumentan. Un ejemplo fue la infección de la red Internet que llegó a Australia antes de poder ser detenida. Esto obliga a que la circulación de información sea igualmente fluida y los conocimientos del fenómeno amplios.

Algunos BBS de Estados Unidos publican boletines con indicaciones sobre nuevos virus, así como alertando sobre falsos programas que son en realidad bombas de tiempo o caballos troyanos.

1.3 Inicios de la regulación de la informática

Históricamente se conocen algunos antecedentes interesantes de declaraciones sobre las libertades del hombre. Antecedentes que influyen sin duda alguna en los inicios de la regulación informática En el siglo XVIII las filosofías políticas convergen en dos documentos básicos para las definiciones de Derechos Fundamentales del hombre y su garantía frente al Estado. El primero es la Declaración de los Derechos del Hombre y del Ciudadano producto de la Revolución Francesa, la cual se

mantiene viva y vigente como texto legal por la remisión que hace el preámbulo de la Constitución de Francia. El segundo de los documentos mencionados con anterioridad. será el de la Constitución de los Estados Unidos de América.

La Declaración de los Derechos del Hombre y del Ciudadano.

En 1789 la Declaración de los Derechos del Hombre y del Ciudadano, presenta una profunda unidad en su inspiración, una destacable coherencia, hasta tal punto que con razón se puede ver en ella un resumen convincente de la filosofía de las luces
En sus artículos X y XI de dicha Declaración de los Derechos del Hombre y del Ciudadano, establece: " Ningún hombre debe ser molestado en sus opiniones ..La libre comunicación de los pensamientos y de las opiniones es uno de los derechos más preciosos del hombre; todo ciudadano puede, pues. escribir e imprimir libremente, salvo la responsabilidad por el abuso de esta libertad en los casos determinados por la ley ." [3]

En 1948 las Naciones Unidas emiten su declaración Universal de Derechos Humanos. En su artículo 12 señala: " Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. "

Así entonces el artículo 19 a la letra dice: " Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones y el de difundirlas, sin limitación de fronteras por cualquier medio de expresión. " [4]
En 1950 un Convenio Europeo para la protección de los derechos Humanos y de las Libertades Fundamentales, manifiesta: " Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o

[3] C. Mejan, Luis Manuel. El Derecho a la Intimidad y la Informática. Porrúa. México 1994 Pp.13-14
[4] C Mejan, Luis Manuel. Op. cit. México 1994 P 14

de comunicar informaciones o ideas sin que pueda haber injerencias de autoridades públicas y sin consideración de fronteras... el ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley... para la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial."[5]

En 1966 la Asamblea General de las Naciones Unidas adopta un Pacto Internacional de Derechos Civiles y Políticos. El Artículo 17 a la letra dice Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, su correspondencia, ni de ataques ilegales a su honra y reputación. (el 20 de mayo de 1981 México ratifico, firmo y se adhirió a este pacto según publicación en el Diario Oficial de la Federación).

La Convención Americana sobre Derechos Humanos, abierta a firma el 22 de noviembre de 1969 y cuya ratificación se público en el Diario Oficial de la Federación el 7 de mayo de 1981 dispone en su artículo 11 la misma ordenanza.

El texto a la letra dice:
Artículo 11.- Protección de la honra y de la dignidad.
1.- Toda persona tiene derecho al respecto de su honor y al reconocimiento de su dignidad.
2.- Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra y reputación

El Convenio pactado entre los miembros del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, tiene un especial significado para nuestro tema, por el hecho mismo de

[5] Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales 1950

haberse producido y que los estados miembros se preocupen por tomar un acuerdo al respecto.
Europa tiene una especial preocupación en este tema dentro del contexto de las estructuras y acuerdos tomados con motivos de los propósitos que se ha fijado la Comunidad Económica Europea.

En el artículo primero del mencionado convenio dice:
Objeto y Fin.- El fin del presente convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente, correspondientes a dicha persona. Es decir su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal.

El contenido del Convenio se desarrolla haciendo una serie de definiciones y de términos, así como de las medidas de seguridad y los derechos de la persona interesada a tener acceso y poder, por lo que si es necesario lograr la modificación de los mismos. Posteriormente aborda el problema del flujo fronterizo de los datos personales. Concluye con una serie de normas orgánicas de la Convención

Este Convenio es un buen modelo para otras regiones del mundo e incluso para los países que están deseosos de producir una normatividad peculiar sobre el tema.

El noviembre de 1989 se adoptó en la Ciudad de Nueva York la Convención sobre los Derechos del Niño, firmado y ratificado por México y publicada en el Diario Oficial de la Federación el 25 de enero de 1991. En este documento sobre los Derechos Fundamentales se dispone·

Artículo 16.- Ningún niño será objeto de injerencias arbitrarias ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. 2.El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

Artículo17.-Los estados Partes reconocen la importante función que desempeñan los medios de comunicación y velarán porque el niño tenga acceso a información y material procedente de diversas fuentes nacionales o internacionales. . e)Promoverán la elaboración de directrices apropiadas para proteger al niño contra toda información y material perjudicial para su bienestar...

La Constitución de los Estados Unidos de América

De la Constitución de los Estados Unidos de América , cabe mencionar que la primera y la cuarta enmienda de 1791 establecen la libertad de expresión y la libertad de prensa, así como la protección a las personas, casas , papeles y posesiones contra molestias sin debida orden.

Siempre ha aparecido una parte dogmática, durante la historia Constitucional Mexicana, que ha contenido tanto la libertad de expresión como la libertad de imprenta, como la garantía de legalidad en las molestias a las propiedades o posesiones. Así durante la misma historia se ha venido observando una aportación de diversas tendencias ideológicas (es decir, ideas de las luchas entre los conservadores y liberales que caracterizaron el siglo XIX en nuestra patria), entrando en vigor así en diversos cuerpos constitucionales pero en todos ellos se da el reconocimiento a tales derechos fundamentales. En la actualidad nuestra Constitución consagra tales garantías.

Para el propósito de nuestro estudio, podemos observar que en algunos otros países consagran otros derechos que invariablemente se encuentran completamente ligados a nuestro tema. Por ejemplo:

Portugal

En Portugal se consagra constitucionalmente el derecho a la intimidad informática y el derecho a la rectificación según se menciona en el artículo 35 que explica:

1.-Todos los ciudadanos tendrán derecho a informarse del contenido de bancos de datos acerca de ellos y de la finalidad a que se destinen las informaciones y podrán exigir la rectificación de los datos, así como su actualización.

2.-Los terceros tendrán prohibido el acceso a archivos con datos personales y a las intercomunicaciones que surjan de ellos así como a los flujos de información transnacionales, salvo en casos excepcionales previstos por la ley.
3.-No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos
4.-La ley determinará el concepto de datos personales para el propósito de bancos de datos.
5.-Los ciudadanos no podrán recibir un número de identificación único usable para todo tipo de propósitos.

En la Constitución portuguesa se consagra en otros artículos 37 y 38, los tradicionales derechos fundamentales a la libertad de expresión, información y prensa en los que se eleva a rango constitucional el derecho a rectificar y replicar También contiene las garantías a inviolabilidad de domicilio y correspondencia y a no ser molestado en sus bienes o personas sin mandamiento legal.

Se encuentra dentro del artículo 26 bajo el titulo de " Otros derechos personales " que a todos les será reconocidos el derecho a su identidad personal, capacidad civil, ciudadanía, buen nombre y reputación, su imagen y el derecho a mantener para sí, reserva de la intimidad de su vida familiar y privada.

En Holanda en su Constitución de 1983, contiene un artículo 10º bajo el título Respeto a la intimidad personal, que dispone la obligación de legislar para la protección de la esfera de la vida personal en relación con la acumulación y suministro de datos personales, así como sobre la responsabilidad de las personas con ocasión del examen de los datos por ellas almacenados y del uso que hicieren de ellos así como el aprovechamiento de tales datos.
En España en el artículo 20 de su Constitución consagra el derecho a comunicar o recibir libremente la información con regulación del secreto profesional en el ejercicio de estas libertades, pero cabe la pena mencionar que en su artículo 18

garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, garantiza también el secreto de las comunicaciones y estipula que la ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos.

En Alemania, en el primer artículo de su Constitución consagra la dignidad misma de la persona o ser humano de la cual se ha establecido jurisprudencialmente que se deriva un derecho a la vida privada. El artículo 5º al consagrar la libertad de opinión establece como uno de los límites que la ley puede imponer dicha libertad, " el derecho del honor personal. "

De esta forma podemos seguir citando más y más constituciones a lo largo de la historia del mundo, que consagren estos derechos fundamentales, pero creo que es suficiente el estudio obtenido, para percatarnos que a través del desarrollo de la humanidad es necesario garantizar, proteger y consagrar dichos derechos fundamentales del hombre.

Dentro de la rapidez con la que avanza la tecnología a través de la informática es necesario y eficaz que dentro del ordenamiento jurídico existan normas de seguridad que permitan el manejo tranquilo y pasivo de este tipo de tecnología. Es por ello que algunos países se han preocupado por esta enorme laguna que existía en el derecho, logrando a veces leyes tan eficaces como obsoletas con la necesidad de cambiarlas o renovarlas.

A continuación se mostraran algunas formas o medidas de seguridad que emplean algunos países para resguardar su derecho a la intimidad. Medidas que tuvieron que emplear desde que el derecho a la intimidad, al secreto profesional se violaron con diversas formas que se manejan con el uso de la tecnología, formas que van desde delitos en contra de la propiedad intelectual, contra la propiedad industrial, por medio de estafas informáticas, sabotajes, fraudes informáticos, en fin un sin número de delitos que hasta hace algunas décadas atrás apenas se comenzaron a legislar,

penalizar y castigar. por las consecuencia tan catastróficas que provocaban inclusive en agencias internacionales.

La cada vez más avanzada tecnología, nos permite darnos cuenta de la sorprendente velocidad con la que las comunicaciones se desarrollan. Modernos sistemas permiten que el flujo de conocimientos sean independientes del lugar físico en que nos encontremos. Ya no nos sorprende la transferencia de información en tiempo real o instantáneo. Se dice que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma publica, se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual es que las organizaciones están uniendo sus redes internas a la Internet, la que crece a razón de más de un 10% mensual.

Al unir una red a la Internet se tiene acceso a las redes de otras organizaciones también unidas. De la misma forma en que accedemos a la oficina de enfrente de nuestra empresa, podemos recibir información de un servidor en Australia, conectarnos a una supercomputadora en Washington o revisar la literatura disponible desde Alemania. Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que puede haber más de uno con perversas intenciones respecto a nuestra organización. Por eso, debemos tener nuestra red protegida adecuadamente.

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos. A pesar de que la prensa ha publicado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. A diario se reciben reportes de ataques a redes informáticas, los que se han vuelto cada vez más siniestros. los

archivos alterados sin aviso alguno, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada y miles de contraseñas han sido capturadas a usuarios inocentes.

Los administradores de sistemas deben de gastar horas y a veces días enteros volviendo a cargar o reconfigurar sistemas comprometidos, con el objeto de recuperar la confianza en la integridad del sistema. No hay manera de saber los motivos que tuvo el intruso y debe suponerse que sus intensiones son lo peor Aquella gente que irrumpe en los sistemas sin autorización, aunque sea solamente para mirar su estructura, causa mucho daño, incluso sin que hubieran leído la correspondencia confidencial y sin borrar ningún archivo.

DISTINTOS NIVELES DE SEGURIDAD DEL DEPARTAMENTO DE DEFENSA DE LOS ESTADOS UNIDOS

El departamento de Defensa de los Estados Unidos ha definido unos niveles de seguridad para sus computadoras, que se recogen en el denominado "Libro Naranja" (por el color de sus tapas), y que es usado como un estándar para indicar el nivel de seguridad de los sistemas informáticos. Estas especificaciones definen siete niveles de seguridad, denominadas A1, B3, B2, B1, C2, C1, D. Siendo el D de menor seguridad y A1 de mayor. Cada nivel incluye las exigencias de los niveles inferiores.

- Nivel D. Estos sistemas tienen exigencias de seguridad mínimos, no se les exige nada en particular para ser considerados de clase D

- Nivel C1. Para que un sistema sea considerado C1 tiene que permitir la separación entre datos y usuarios, debe permitirse a un usuario limitar el acceso a determinados datos, y los usuarios tienen que identificarse y validarse para ser admitidos en el sistema

Nivel C2. Para que un sistema sea de tipo C2 los usuarios tienen que poder admitir o denegar el acceso a datos a usuarios en concreto, debe de llegar una

auditoría de accesos, e intentos fallidos de acceso a objetos (archivos, etc.), y también especifica que los procesos no dejen residuos (datos dejados en registros, memoria o disco por un proceso al "morir").

- Nivel B1. A un sistema de nivel B1 se le exige control de acceso obligatorio, cada objeto del sistema (usuario o dato) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

- Nivel B2. Un sistema de nivel B2 debe tener un modelo teórico de seguridad verificable, ha de existir un usuario con los privilegios necesarios para implementar las políticas de control, y este usuario tiene que ser distinto del administrador del sistema (encargado del funcionamiento general del sistema). Los canales de entrada y salida de datos tienen que estar restringidos, para evitar fugas de datos o la introducción de éstos.

- Nivel B3. En el nivel B3 tiene que existir un argumento convincente de que el sistema es seguro, ha de poderse definir la protección para cada objeto (usuario o dato), objetos permitidos y cuales no, y el nivel de acceso permitido a cada cual Tiene que existir un "monitor de referencia" que reciba las peticiones de acceso de cada usuario y las permita o las deniegue según las políticas de acceso que se hayan definido. El sistema debe ser muy resistente a la penetración de intrusos, así como tener una auditoría que permita detectar posibles violaciones de la seguridad.

- Nivel A1. Los sistemas de nivel A1 deben cumplir los mismos requerimientos que los de nivel B3, peor debe ser comprobado formalmente el modelo de seguridad definido en el nivel B3.

ALGUNOS CASOS QUE REGULAN A LOS DELITOS INFORMATICOS

Algunos de los países que se preocuparon por mantener el orden dentro de la tecnología informática, para bienestar de su comunidad son los siguientes:

-El 28 de septiembre del dos mil, la Agencia de Protección de Datos multa a Telefónica La Agencia de Protección de Datos (APD) ha considerado que Telefónica fue culpable de una falta grave al exponer en Internet datos de facturación de sus clientes. La multa aplicada, de diez millones de pesetas, es la sanción mínima que recoge la ley para este tipo de casos.

Desde Hispasec dimos a conocer esta información el pasado mes de febrero. El problema provenía de un fallo de programación y configuración del servidor web En principio, para acceder a este servicio, que es público y está al alcance de cualquier internauta que pase por el web de Telefónica, es necesario un nombre de usuario y contraseña, tal y como se informa en las páginas web del operador. Pero resultaba relativamente sencillo saltarse esta protección, por lo que cualquier usuario podría llegar a conocer la facturación detallada, incluyendo datos como el domicilio bancario, con tan sólo introducir el número de teléfono sobre el que se deseaba obtener información.

La resolución de la APD considera probado que durante varios días el directorio de navegación donde se recogía la existencia de la página para accesos internos figuró visible y accesible desde Internet Así como que el pasado 25 de febrero se produjeron 829 accesos no autorizados a datos de facturación de los abonados de Telefónica, llegando a los 6.330 accesos el día 28, si bien se incluye en la cifra los accesos del propio personal de Telefónica.

A juicio de la Asociación de Internautas, es "insuficiente" que a la vista de todos estos hechos se imponga una multa que podríamos calificar de irrisoria, si tenemos en cuenta el potencial de la compañía sancionada.

-El pasado 21 de septiembre, Erkki Liikanen, comisario de Empresa y Sociedad de la Información, ha dado a conocer los principios en los que se basará la Unión Europea para luchar contra los delitos que se realicen en Internet El comisario informó que se

potenciará la formación de los usuarios, se incrementarán las medidas de seguridad en la red, y se fomentará la cooperación internacional.
Para aplicar esta política se tipifican los delitos en dos grandes grupos, en el primero se parte de la base de que los delitos que se cometen fuera de Internet, lo son también si se realizan dentro de la red. Separados en un segundo apartado se encuentran los delitos propios de las nuevas tecnologías, cómo el "cracking" y los virus informáticos.

Erkki Liikanen comentó que en la actualidad existen numerosos sistemas para proteger la información de nuestros sistemas, pero el problema viene por el uso insuficiente de estas herramientas. "El cifrado es la mejor herramienta para la transmisión de datos y el comercio. Ya tenemos la tecnología, solo hace falta que la gente aprenda a usarla".

Igualmente, el pasado día 21 se aprobaron también una serie de enmiendas sobre la competencia de tribunales en demandas relativas a las transacciones realizadas vía electrónica. Con estas enmiendas se establece un ámbito de actuación por el cual un usuario podrá interponer una demanda en su país de origen relativa a transacciones electrónicas realizadas con una empresa de otro país de la Comunidad Europea.

En este mismo marco se presentó otra enmienda en la que se aboga por uso más extensivo de las vías extrajudiciales para la resolución de los conflictos sobre transacciones electrónicas, ya que la utilización de medios judiciales ralentizan y encarecen de manera especial los procesos cuando las partes implicadas en los procesos tienen como domicilio diferentes Estados de la Unión Europea.

1 de octubre del dos mil. El Senado argentino ha dado un importante paso adelante para la protección del derecho a la intimidad de sus ciudadanos, al aprobar una ley que tendrá como fin garantizar a los ciudadanos el control y el libre acceso a la información que de estos posean organismos públicos y privados

Tras un largo período que data de la reforma constitucional realizada en 1994, en la cual se establecía en su artículo 43 el derecho de cualquier ciudadano a preservar su intimidad, y tras enfrentarse incluso a un veto presidencial en 1996, el pasado día 4 del presente mes fue aprobada la ley denominada "Hábeas Data".
Esta ley se encargará de proteger los datos de los ciudadanos argentinos.
La citada ley distingue dos tipos de datos, los comunes (nombre, apellidos, dirección, etc.) y los sensibles.
Se consideran como datos sensibles cualquier información del individuo que pueda motivar algún tipo de discriminación por parte de terceros. Entre estos últimos estarían la raza y la orientación política o sexual.

La nueva ley obliga a las empresas a comunicar por escrito a los ciudadanos la inclusión de sus datos personales en sus bases de datos De igual forma se establece la obligatoriedad de suprimir o sustituir los datos inexactos de cualquier ciudadano. Los datos de los ciudadanos deberán ser fácilmente accesibles por los mismos, para ello se establece un plazo de 10 días para responder a la consulta de información de cualquier individuo que previamente haya demostrado su identidad

Para controlar esta ley se crea un nuevo organismo de control estatal cuya misión será la de vigilar a los organismos públicos y empresas privadas Este órgano podrá aplicar multas que van desde lo 5 000 hasta los 100.000 pesos a quien o quienes ofrezcan información sin consentimiento o errónea. Incluso, se podrá llegar a condenas de 3 años de prisión si se incluyen datos falsos a sabiendas.

CAPITULO II CONCEPTO DE DELITO Y DEFINICIONES DE DELITO INFORMÁTICO

2.1 Definición de delito informático

Antes de entrar directamente en materia y mostrar las distintas definiciones del delito informático, presentaremos la definición de delito según el Código Penal federal vigente, para tener una ubicación de lo es delito según el derecho.

Artículo 7 - Delito es el acto u omisión que sancionan las leyes penales

En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar precedente.

El delito es:

Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos;

Permanente o continuo, cuando la consumación se prolonga en el tiempo, y

Continuado, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal

Una definición propia del delito informático a nivel internacional se puede pensar que no existe aún. Considerando el enorme esfuerzo que los especialistas en la materia han realizado lentamente, se ha podido lograr ésta labor de crear conceptos o definiciones atendiendo a la situaciones reales que en el mundo de la informática adolece. " De esta manera que dar un concepto sobre delitos informáticos no es una labor fácil y esto es en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de `delitos´ en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión `delitos informáticos´ este consignada en los códigos penales, lo cual en nuestro

país. al igual que en muchos otros, no ha sido objetos de tipificación aún [6], mientras muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

Para el autor Davara Rodríguez no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Definiendo de esta manera al delito informático como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Determinados enfoques doctrinales subrayan que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

De esta manera, el autor mexicano Julio Tellez Valdez , señala que los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)

Según TELLEZ VALDEZ, en su obra " Delitos Informáticos ", 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.

[6] Tellez Valdez, Julio. Derecho Informático Editorial Mc Graw-Hill México. 1996 Pp 103-104

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

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

Por otra parte, cabe mencionar que se han formulado diferentes denominaciones además de delitos informáticos, para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos electrónicos, delincuencia informática, delincuencia de cuello blanco, abuso informático, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el

ordenador, etcétera. De tal manera que haciendo alusión de lo anterior se darán sólo algunos de estos conceptos como mera referencia.

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

Gómez Perals, define a la delincuencia informática como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

La doctrina, casi unánimemente , la considera inscribible en la criminalidad de Cuello Blanco. Para Sutherland, la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.

Ruiz Vadillo, recoge la definición que adopta el mercado de la OCDE en la Recomendación número R(81) 12 del Consejo de Europa, indicando que abuso informático es " todo comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos. "[7]

A) SUJETOS ACTIVOS

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

[7] Ruiz, Vadillo Enrique Tratamiento de la delincuencia Informática como una de las expresiones de criminalidad económica Poder Judicial numero especial IX Madrid, España. 1989

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 "ingresa" 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

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

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

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

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las

cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios. entre otros.

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. Sin embargo, la cifra 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.

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. Estas son:

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 se 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.

B) SUJETOS PASIVOS

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

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

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

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

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

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

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y

estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

2.2 Clasificación de Delito Informático.

En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y la telemática, y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito: una finalidad deseada que causa un perjuicio a otro, o a un tercero

María de la Luz Lima, en su obra titulada " Delitos Electrónicos ", presenta una clasificación, de los mismos, diciendo que existen tres categorías, a saber:

1.- Los que utilizan la tecnología electrónica como método,

Como método.- Conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

2.- Los que utilizan la tecnología electrónica como medio.

Como medio.- Conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.

3.- Los que utilizan la tecnología electrónica como fin.

Como fin.- Conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Ahora bien en la obra " Interacción del Derecho y la Informática " de Barriuso Ruiz , los delitos informáticos los podemos clasificar en: 1) Delitos contra la intimidad, 2) De los robos, 3) De las estafas, 4) De las defraudaciones, 5) De las daños, 6) Relativo a la protección de la propiedad industrial, 7) Relativo al mercado y a los consumidores.

En cuanto al autor Pérez Luño, en su ' manual de informática y derecho " que él realizo, podemos hacer la siguiente clasificación·

a) Desde el punto de vista subjetivo.

Ponen el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuestos de criminalidad

b) Desde el punto de vista objetivo.

Considerando los daños económicos perpetrados por las conductas criminalistas sobre los bienes informáticos, es decir:

Los fraudes:

1.- Manipulaciones contra los sistemas de procesamiento de datos Podemos citar:

- Los daños engañosos (data diddling)
- Los caballos de troya (troya horses)
- La técnica del salami (salami technique/rounching down)

2.- El sabotaje informático:

- Bombas lógicas
- Virus informáticos

3.- El espionaje informático y el robo o hurto de software:

- Fuga de datos (data leakage)

4.-El robo de servicios:

- Hurto del tiempo del ordenador
- Apropiación de informaciones residuales (scavenging)
- Parasitismo informático (piggybacking)
- Suplantación de personalidad (impersonation)

5.-El acceso no autorizado a servicios informáticos:

- Las puertas falsas (trap doors)
- La llave maestra (superzapping)
- Pinchado de líneas (wiretapping)

c) Funcionales.

La insuficiencia de los planteamientos subjetivos y objetivos han aconsejado primar otros aspectos que puedan resultar más decisivos para delimitar la criminalidad informática. Atentados contra la fase de entrada (input) o de salida (output) del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.

Para Baón Ramírez dentro de la criminalidad informática podemos distinguir dos grandes grupos de delitos:

1 - El primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así distinguiremos los delitos:

- Relativos a la destrucción o sustracción de programas o de material.
- Relativos a la alteración, destrucción o reproducción de datos almacenados.
- Los que se refieren a la utilización indebida de ordenadores.

2.- En un segundo grupo se encuadraría la comisión de los delitos más tradicionales como los delitos contra:

- La intimidad
- La propiedad
- La propiedad industrial o intelectual
- La fe pública
- El buen funcionamiento de la administración
- La seguridad exterior e interior del Estado
- En la obra " Derecho Informático " de Davara Rodríguez, se hace una distinción de la manipulación mediante la informática en dos vertientes diferentes:

a) Acceso y manipulación de datos.
b) Manipulación de los programas.

Atendiendo a ello, se considera que determinadas acciones que se podrían encuadrar dentro de lo que hemos llamado el delito informático, y que para su estudio, las clasifica. de acuerdo con el fin que persiguen, en seis puntos.

1 - Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.

2.- Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

3.- Introducción de programas o rutinas en otros ordenadores para destruir información , datos o programas.

4.- Utilización del ordenador y/o los programas de otras personas. sin autorización con el fin de obtener beneficios propios y en perjuicio de otro.

5 -Utilización del ordenador con fines fraudulentos.

6.- Agresión a la "privacidad" mediante la utilización y procesamiento de datos personales con fin distinto al autorizado

Julio Téllez Valdes en su obra antes citada, clasifica a los delitos informáticos en base a dos criterios· como instrumento o medio. o como fin u objetivo.

1 - Como instrumento o medio

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

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

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

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

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

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

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

l.- Acceso a áreas informatizadas en forma no autorizada

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

2.- Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

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

b - Destrucción de programas por cualquier método

c - Daño a la memoria

d.- Atentado físico contra la máquina o sus accesorios.

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

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

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

- Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.

- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

-Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos: Espionaje· Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Como nos hemos podido dar cuenta y conforme a lo escrito anteriormente existen distintos tipos de clasificación de acuerdo al autor y a la situación jurídica en la que se encuentra determinado país. Independientemente de que todas estas clasificaciones antes presentadas son parecidas, de tal forma que podríamos tomarlas como una sola clasificación y utilizarla para nuestro estudio, esto no es posible debido a que como lo señale antes depende de la situación jurídica de cada país, para llevar a cabo una clasificación del delito informático Por lo que para nuestro estudio tomaremos en cuenta la clasificación que nos presenta el autor mexicano Julio Tellez Valdes, ya que las clasificaciones anteriores solo se tomaron como mera referencia para darnos cuenta de la diferencia que existe entre una clasificación que plantea un país que encuadra los delitos informáticos en su legislación, y otra clasificación en la que su país se encuentra con la necesidad de legislar dichos delitos.

2.3 Tipos de Delitos informáticos

Los tipos de delitos informáticos reconocidos por las Naciones Unidas. [8]

1.- Fraudes cometidos mediante manipulación de computadoras.

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

[8]Naciones Unidas. Revista Internacional de Política Criminal Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos Oficina de las Naciones Unidas en Viena. Centro de desarrollo Social y Asuntos Humanitarios Naciones Unidas, Nueva York 1994 Números 43 y 44

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

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años. El autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otros

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

Al respecto se especificarán y explicarán las distintas formas de manipulación de datos o programas que existen, en la informática.

Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya

que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

La manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2.- Falsificaciones informáticas.

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

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

3.- Daños o modificaciones de programas o datos computarizados.

Sabotaje informático El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o software de un sistema Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente podríamos diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

El primer grupo comprende todo tipo de conductas destinadas a la destrucción física del hardware y del software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes caústicos en los equipos, etcétera). En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos.

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos lógicos, o sea, todas aquellas conductas que producen, como resultado la destrucción, ocultación o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas Desde la más simple que podemos imaginar (como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.
Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces en forma combinada. Las técnicas que permiten cometer sabotajes informáticos son:

VIRUS. Es una serie de claves programadas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya que aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos.

Es un programa de ordenador que se reproduce así mismo e interfiere con el *hardware de una computadora* o con su *sistema operativo* (el software básico que controla la computadora). Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo

Como se producen las infecciones.
Los virus informáticos se difunden cuando las instrucciones - o código ejecutable- que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informática. Estas infecciones son mucho más frecuentes en PC que en sistemas profesionales de

grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan Por eso. si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático para que ejecute el programa viral.

Algunos virus tienen la capacidad de adherirse a programas legítimos Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, lo mismo ocurre con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

Especies de virus

Existen seis categorías de virus: parásitos, del sector de arranque inicial, multipartitos, acompañantes, de vínculo y de fichero de datos. Los virus parásitos infectan ficheros ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa. Los virus del sector de arranque inicial residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el

ordenador Estos virus suelen difundirse mediante el intercambio físico de discos flexibles. Los virus multipartitos combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus. Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas característica y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de ficheros de datos, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo

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

BOMBA LÓGICA O CRONOLÓGICA. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento

dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba. Es decir, una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras.

4.- Acceso no autorizado a servicios y sistemas informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos. desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

5.- Piratas informáticos o hackers.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo. los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

HACKERS.

Hack. Corte, hachazo, tajo, puntapié, mella. Collins Dictionary, Ingles-Español. La definición más comúnmente asociada al término hacking hoy día es intrusión sigilosa en un sistema informático sin autorización.

Y según otros expertos, la palabra deriva de hack, un término que se usaba para describir la familiar forma en que los técnicos telefónicos arreglaban cajas defectuosas; el viejo pero efectivo golpe seco La persona que realizaba esa operación era, naturalmente, un hacker. Independientemente de la raíz etimológica de la palabra, lo que sí parece objeto de consenso es que serían los estudiantes del famoso MIT (Masachusetts Institute of Technology) los que acercaran la acepción del término a una definición en la que se incluían ordenadores.

Efectivamente, ya en 1959 algunos estudiantes se reunían a través de un ordenador IBM 407 Por aquél entonces, era común que el ordenador fallase por razones extrañas y las reparaciones consistían a veces en aplicar un buen golpe en el costado del ordenador: un método de sorprendente eficacia para la tecnología a base de válvulas de la época.

Según la definición de "The New Hackers Dictionary" de Eric Raymond, los hackers son inteligentes, intensos, abstraídos e intelectualmente abiertos. Se interesan por cualquier sujeto que les pueda proporcionar estimulación mental y es común que tengan una afición extrema al hacking, en el que se desenvuelven competentemente. Les encanta el control, pero no en forma autoritaria sino sobre cosas complicadas, como las computadoras. Se apasionan por lograr que esas máquinas sean instrumentos de lo interesante, siempre y cuando se trate de sus propias ideas y no de una orden de alguien. No les gustan las rutinarias tareas cotidianas que llevan a mantener una existencia normal; por ello, si bien son ordenados en sus vidas intelectuales, son caóticos en el resto. Prefieren el desafío del conocimiento a una recompensa monetaria por un trabajo.
Aparte de los hackers, nos encontramos con otra serie de términos de sonido similar aunque conviene aclarar las diferencias.
Otro tipo de individuos son los crackers, siempre en el ámbito de las redes informáticas, considerados como una especie de "hackers destructivos". Penetran en los sistemas y ocasionan daños deliberadamente. A veces también son denominados como crashers (de crash: rotura, aniquilación).

Los hackers se sirven de una amplia gama de artimañas para conseguir colarse en un sistema Pueden acudir a la denominada "ingeniería social", que consiste en ganarse la confianza de alguna persona que, por trabajar en el entorno del sistema, posee la información necesaria para abrirse la puerta de entrada al mismo. Obviamente, la "ingeniería social" es todo un arte y el "ingeniero" ha de ser cuidadoso para no caer o, de lo contrario podría convertirse en un "sospechoso habitual" ante cualquier anomalía o incursión que fuera detectada en adelante en ese sistema.

Otro método a utilizar son los Caballos de Troya, es decir, programas que se introducen en el ordenador y, engañando al usuario (que puede ser incluso el administrador del sistema) consiguen determinados datos de gran utilidad para el hacker.

Un caballo de Troya típico es aquel que imita el proceso de entrada a un sistema. Consiste en un programa que presenta la típica pantalla de login (usuario) y password (contraseña) para entrar en el sistema. El usuario no nota diferencia alguna y, contento y feliz, escribe ambos, uno detrás de otro.. pero estos irán a parar a un fichero del que serán "recolectados" más tarde por el hacker. Como realmente no se ha entrado en el sistema, el caballo de Troya simulará un mensaje de "password incorrecto" excusa bajo la cual, esta vez si invocará la verdadera rutina de entrada al sistema. El usuario (víctima) pensará "juraría que lo escribí correctamente. Bueno, al segundo intento lo consigo".

Lo cierto, es que la mayoría de las veces, lo más fácil es explotar los agujeros que tiene un sistema en particular. Las primeras averiguaciones pueden consistir en conocer que tipo y que versión de sistema operativo corren en la máquina en cuestión. Este dato es muy importante ya que cualquier hacker que se precie, estará al tanto de los "bugs" o agujeros de seguridad que son explotables en esa versión de sistema operativo en cuestión.

TÉCNICAS DE LOS HACKERS.

No solo las redes conectadas a Internet son vulnerables a los ataques de los hackers. El método más común de acceder ilegalmente a un sistema es a través de

una terminal de la propia red de la organización. Cualquier persona con acceso físico a una terminal tiene la oportunidad de ingresar.
En caso de acceso remoto, por teléfono, también es posible de ingresar al sistema, aún sin conexión a Internet. Existen varios programas computacionales de discado telefónico automático o reiterativo, con los cuales se puede identificar él numero de teléfono conectado al un módem, si se le da un rango de números a probar Normalmente, dicho número es parecido al de la empresa en cuestión.

Una vez que se tiene acceso a la organización será necesario obtener una combinación válida de nombre de usuario y contraseña. Los hackers pueden intentar un ataque manual o automático para averiguar contraseñas válidas, mediante programas sencillos disponibles en Internet. Muchos sistemas guardan sus cuentas de usuario y las contraseñas correspondientes en un archivo especial protegido por encriptación. Si un hacker accede a dicho archivo puede descifrarlo con un programa como el "crack", en el caso de sistemas UNIX, el cual compara las palabras del diccionario, encripatadas, con el contenido de dicho archivo, hasta encontrar coincidencias.

Un hacker puede instalar en una estación del sistema un pequeño programa de captura la secuencia de teclas digitadas. Es el denominado "Caballo de Troya , y actúa solapadamente capturando y guardando en un archivo todo lo que se digita después de ciertas palabras claves como "login", "username", "nombre", "password", "contraseña", etcétera. Posteriormente, el hacker revisa desde un lugar remoto el contenido del archivo que obtuvo. Esta técnica es relativamente simple, y generalmente nadie nota nada.

En Internet se pueden encontrar una amplia variedad de herramientas para monitorear y analizar redes, llamadas "packet sniffers", las que actúan revisando los paquetes de información electrónica que transitan por una determinada red Como generalmente dichos paquetes de una red no están encriptados, bastará revisar

dicha información, especialmente entre las 8 y 9 A.M. para conocer nombres de usuarios y sus contraseñas.

En el caso de redes conectadas a la Internet, los hackers pueden alterar su identidad, haciendo creer a la computadora que da acceso a una determinada identidad y a una determinada institución, que son computadoras "autorizadas" a ingresar o confiables.

6.- Reproducción no autorizada de programas informáticos de protección legal.
La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

CAPITULO III MARCO JURÍDICO

3.1 Título noveno del Código Penal Federal.

Cabe la pena mencionar las distintas etapas por las que a atravesado la denominación de nuestro cuerpo legal punitivo en una breve remembranza y así, una vez explicado poder entrar en la materia que nos concierne.

A lo largo de la historia de nuestra legislación mexicana y de la legislación internacional, se han encontrado diversas disposiciones con el propósito de regular la conducta del hombre, para así poder convivir en armonía y en beneficio de la sociedad. Es a través del tiempo, de las costumbres y de la tecnología (con la que el hombre se ha caracterizado por perfeccionar), como las necesidades del mismo van creciendo, de modo que es imperativo e importante crear legislaciones y procedimientos que regulen las distintas actividades del ser humano, de manera que el progreso con el que el hombre se va desarrollando sea conforme a derecho y con las regulaciones que está ofrece.

De esta manera aún siguen vigentes los principios que dieron lugar al nacimiento del Código Penal de 1931, denominado Código Penal para el Distrito y Territorios Federales, en materia de Fuero Común y para toda la República, en materia Federal. Este ordenamiento fue promulgado el 13 de agosto de 1931, y empezó su vigencia el 17 de septiembre siguiente. Pero fue el Presidente Constitucional de los Estados Unidos Mexicanos, el que en uso de sus facultades que le fueron concedidas por decreto de 2 de enero de 1931, expidió el Código Penal para el Distrito y Territorios Federales, en materia de Fuero Común y para toda la República, en materia Federal. De esto se desprende que entonces dicho Código no fue resultado de una labor legislativa. " Dichos principios que dieron vida a este ordenamiento siguen vigentes, pues podemos observar que no es una teoría, ni una escuela jurídica las que van a dar respuesta a las necesidades de contar con un Código Penal adecuado para el Distrito Federal, es recogiendo la práctica y

utilizando los métodos idóneos que podrá combatirse de mejor manera a la delincuencia mediante un sistema jurídico ordenado [9]

Así pues, dicho ordenamiento cambio de denominación, quedando entonces como Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, todo esto debido a que desaparecieron los territorios federales, convirtiéndose en Estados Libres y Soberanos

Es mediante el decreto publicado el 18 de mayo de 1999, cuando el legislador federal, cambia de nombre nuevamente al mencionado Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, por la denominación de Código Penal Federal, por así requerirlo necesario

Por ello es que la Asamblea Legislativa del Distrito Federal, I legislatura, decreta para así publicar el 17 de septiembre de 1999 la nueva denominación que se le haría al Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, por la de Código Penal para el Distrito Federal y que entraría en vigor el 1 de octubre de 1999

ANTECEDENTES DE LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS, EN EL CÓDIGO PENAL FEDERAL.

La importancia de llevar a cabo para poder concretarse una iniciativa de ley que regule los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito, se ve reflejada de cierta forma en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Tal fue la necesidad de los legisladores de ocuparse de las conductas que podían tipificarse como delitos y determinar las sanciones para así poder evitar su comisión,

[9] Codigo Penal. Exposicion de Motivos Comentarios Lic Efrain Garcia Ramirez. Editorial Sista México 2000 COM-4

ESTA TESIS NO SALE DE LA BIBLIOTECA

que consideraron que dicha iniciativa de ley (Ley Federal del Derecho de Autor) no abarcaba los tipos penales del delito, por lo tanto se presentó otra iniciativa de Decreto de Reforma al Libro Segundo del Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, proponiendo la adición de un Título Vigésimo Sexto, denominado " De los delitos en materia de derechos de autor", ante la Cámara de Diputados y el 24 de diciembre de 1996, se público en el Diario Oficial de la Federación el mencionado decreto de reforma, entrando en vigor el 25 de diciembre de 1996. En dicho Título se encuentran los artículos 424, 425, 426, 427, 428 y 429. Artículos que más adelante se expondrán con detenimiento.

Por decreto publicado en el Diario Oficial de la Federación el 19 de mayo de 1997 se reforman la fracción III del artículo 231 de la Ley Federal de Derechos de Autor, así como la fracción III del artículo 424 del Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal.

De esta manera y a raíz de las intromisiones de que han sido objeto diversos sitios Web del gobierno federal, como la pagina de la Secretaria de Hacienda y Crédito Publico, y posteriormente la red del Senado de la República, los legisladores mexicanos se abocaron desde mediados de noviembre de 1999, a la tarea de articular una reforma legislativa y punitiva, que en el corto plazo permitiera la prevención y penalización de esta conducta en el ámbito local. Así pues como resultado de este ejercicio, fue aprobada mayoritariamente por la Cámara de Senadores esta miscelánea penal mediante la cual se propuso ante esa representación, la incorporación de un novedoso y breve titulo a nuestro de por si desfasado Código Penal.

Es un apartado que regula y penaliza el acceso ilegal a los sistemas y equipos de cómputo tanto públicos como privados; así como de la tutela y protección de la información oficial, comercial y personal, contenida en dichas computadoras.

Por lo que el 17 de mayo de 1999 se pública en el Diario Oficial, la adición de el Capítulo II del Título Noveno, libro segundo los artículos 211Bis 1, 211Bis 2, 211Bis 3, 211Bis 4, 211Bis 5, 211Bis 6 y 211Bis 7 al Código Penal, entrando así en vigor el 18 de mayo de 1999.

Ahora bien, como se señalo anteriormente el 18 de mayo de 1999, la denominación del Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, cambió por la de Código Penal Federal, dentro de la cual como lo señala su título contiene disposiciones de carácter federal Por lo que el decreto publicado en la Gaceta Oficial del Distrito Federal y en el Diario Oficial de la Federación, el 17 y 19 de septiembre de 1999, se derogan los artículos 424, 425, 426, 427, 428 y 429, pertenecientes al Libro Segundo del Título Vigésimo Sexto, denominado ' De los delitos en materia de derechos de autor ". del Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal, ya que la naturaleza de dichos artículos corresponde a ordenamientos de carácter federal, por lo que debe y tiene que encuadrarse estas disposiciones en el Código Penal Federal, así de esta manera al momento de realizar dicha derogación, queda claro que este tipo de preceptos se establecen dentro de la materia federal, por lo que desde ahora estará regida y regulada en el Código Penal Federal.

Sin más preámbulo y después de explicar las diversas reformas que sufrió nuestro Código Penal Federal, se presentará a continuación los artículos que regulan los delitos informáticos mencionando claro está todos los ordenamientos que se encuentren encuadrados en este Código Penal Federal. Quedando de esta manera:

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPITULO II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 Bis-1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos

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

Artículo 211 Bis-2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado protegidos por algún mecanismo de seguridad, se le impondrán de un año a cuatro años de prisión, y de doscientos a seiscientos días multa Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a dos años de prisión, y de cien a trescientos días multa

Artículo 211 Bis-3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrá de dos a ocho años de prisión, y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrá de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 Bis-4 Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se les impondrán de seis meses a cuatro años de prisión, y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenidas en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegido por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 Bis-5. Al que estando autorizado para accesar a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión, y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrá de tres meses a dos años de prisión, y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementan en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

Artículo 211 Bis-7. Las penas previstas en este capítulo se aumentarán hasta una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

TITULO VIGÉSIMOSEXTO

De los Delitos en materia de derechos de autor.

Artículo 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;

II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien use en forma dolosa, con fin de lucro y sin autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

Artículo 424-Bis. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 424 Ter. Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias obras, fonogramas, videogramas o libros, a los que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales o de manera organizada o permanente, se estará lo dispuesto en el artículo 424 Bis, de este Código.

Artículo 425. Se impondrá una prisión de seis meses a dos años de trescientos a tres mil días de multa, al que sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426. Se impondrá una prisión de seis meses a cuatro años y de trescientos a tres mil días de multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa, a quien publique a sabiendas una obra substituyendo el nombre del autor por otro nombre.

Artículo 428. Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley federal del Derecho de Autor.

Artículo 429. Los delitos previstos en este título se perseguirán por querella de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguida de oficio. En el caso de que los derechos de autor hayan entrado al dominio público, la querella la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

Transitorio Cuarto.- Las referencias que en el presente decreto se hagan al Código Penal para el Distrito Federal en materia del fuero Común y para toda la república en Materia de fuero Federal, se entenderán hechas al Código Penal Federal.

Todas estas deficiencias e imperfecciones se derivan principalmente del limitado y rebasado procedimiento parlamentario tradicional.

En cuanto a las reformas hechas al Título Noveno, podemos observar que las expectativas generadas por la publicación de este ordenamiento, evidentemente, superaron su contenido y aplicación práctica, el cuál involuntariamente representa

apenas un avance en cuanto a la estructuración del piso mínimo a partir del cual los integrantes de la próxima legislatura federal, simultáneamente y en coordinación con los parlamentos de nuestros principales socios comerciales, deberán definir, tipificar y reglamentar la figura de los delitos informáticos. Así en relación a las reformas consagradas al Título Vigésimo Sexto, se puede determinar que dichos ordenamientos como lo aclara la denominación de su capítulo, son en materia de derechos de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, y de tal manera y conforme a la Ley Federal del Derecho de Autor se encuentran regulados los programas de computación y las bases de datos protegidos en la misma forma que una obra literaria, por lo que es indispensable y necesario dejar claro que las consecuencias realizadas por los delitos informáticos, además de estar protegidas por los derechos de autor, su bien jurídico a tutelar serán también la intimidad, seguridad patrimonial, fe pública, honor, dignidad, en fin, situaciones que nuestra legislación mexicana todavía no protege, por lo que aún no se encuentra especificado un procedimiento en el Código Penal, de tal manera que no existe un procedimiento adecuado al cuál acudir para sancionar y perseguir dichos delitos. Problemática que abordaré en el capítulo cuarto, punto número 4.3 del presente trabajo de investigación.

3.2 Ley Federal del Derecho de Autor.

Respecto a esta Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997, se mencionan y explican a continuación por orden de aparición los artículos que nos ocupa solamente a nuestro tema en particular, que se encuentran en el Título IV DE LA PROTECCIÓN AL DERECHO DE AUTOR, en su Capítulo IV De los programas de computación y las bases de datos

TITULO IV

De la protección al Derecho de autor

CAPÍTULO IV

De los programas de computación y las bases de datos

Artículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una

secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 33. A falta de estipulación expresa, toda transmisión de derechos patrimoniales se considera por el término de 5 años. Sólo podrá pactarse excepcionalmente por más de 15 años cuando la naturaleza de la obra o la magnitud de la inversión requerida así lo justifique.

Artículo 104. Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 27. Los titulares de los derechos patrimoniales podrán autorizar o prohibir:

I..., II..., III..., IV. La distribución de la obra, incluyendo la venta u otras formas de transmisión de la propiedad de los soportes materiales que la contengan, así como cualquier forma de transmisión de uso o explotación. Cuando la distribución se

lleve a cabo mediante la venta, este derecho de oposición se entenderá agotado efectuada la primera venta, salvo en el caso expresamente contemplado en el artículo 104 de esta ley; . . . .

Artículo 105. El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando.

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106 El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107. Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108. Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109. El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate. Quedan exceptuadas de lo anterior las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110. El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación,

III La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111 Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta ley en los elementos primigenios que contengan.

Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la

protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta ley.

Artículo 114. La transmisión de obras protegidas por esta ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

3.3 Sexta parte, Capítulo XVII, del Tratado de Libre Comercio de América del Norte.

Este tratado fue suscrito y firmado por el Gobierno de México, por el de los Estados Unidos de América y por el de Canadá en 1993, contiene un apartado sobre propiedad intelectual que se encuentra en la Sexta parte, Capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimiento de ejecución.

De tal manera que a continuación daremos a conocer en términos generales los artículos relativos a nuestro tema que contiene dicho tratado, comprendidos en la sección de la propiedad intelectual, misma que corresponden a nuestra materia, para que así nos demos una idea de lo que este instrumento internacional a aportado a la realización de una posible regulación de los delitos informáticos en México.

SEXTA PARTE PROPIEDAD INTELECTUAL

Capítulo XVII Propiedad intelectual

Artículo 1701. Naturaleza y ámbito de las obligaciones

. Cada una de las Partes otorgará en su territorio, a los nacionales de otra Parte. rotección y defensa adecuada y eficaz para los derechos de propiedad intelectual,

asegurándose a la vez de que las medidas destinadas a defender esos derechos no se conviertan en obstáculos al comercio legítimo.

2. Con objeto de otorgar protección y defensa adecuada y eficaz a los derechos de propiedad
intelectual, cada una de las Partes aplicará, cuando menos, este capítulo y las disposiciones sustantivas de:
a) El Convenio de Ginebra para la Protección de los Productores de Fonogramas Contra la Reproducción no Autorizada de sus Fonogramas, 1971 (Convenio de Ginebra);
b) El Convenio de Berna para la Protección de Obras Literarias y Artísticas, 1971 (Convenio de Berna);
c) El Convenio de París para la Protección de la Propiedad Industrial, 1967 (Convenio de París); y
d) El Convenio Internacional para la Protección de las Obtenciones Vegetales, 1978 (Convenio UPOV), o la Convención Internacional para la Protección de Nuevas Variedades de Plantas, 1991 (Convenio UPOV).
Las Partes harán todo lo posible para adherirse a los textos citados de estos convenios si aún no son parte de ellos a la fecha de entrada en vigor de este Tratado.

3. El Anexo 1701.3 se aplica a las Partes señaladas en ese anexo

Artículo 1702. Protección ampliada

Cada una de las Partes podrá otorgar en su legislación interna protección a los derechos de propiedad intelectual más amplia que la requerida en este Tratado, siempre que tal protección no sea incompatible con este Tratado.

Artículo 1703. Trato nacional

Cada una de las Partes otorgará a los nacionales de otra Parte trato no menos favorable del que conceda a sus propios nacionales en materia de protección y

defensa de todos los derechos de propiedad intelectual. En lo que se refiere a los fonogramas, cada una de las Partes otorgará a los productores y artistas intérpretes o ejecutantes de otra Parte dicho trato, excepto que cada una de las Partes podrá limitar los derechos de los artistas intérpretes o ejecutantes de otra Parte respecto a los usos secundarios de sus fonogramas, a los derechos que sus nacionales reciban en el territorio de esa otra Parte.

2. Ninguna de las Partes podrá exigir a los titulares de derechos, como condición para el otorgamiento de trato nacional conforme a este artículo, que cumplan con formalidad o condición alguna para adquirir derechos de autor y derechos conexos.

3. Cada una de las Partes podrá hacer excepción de lo señalado en el párrafo 1, respecto a sus procedimientos administrativos y judiciales para la protección o defensa de los derechos de propiedad intelectual, inclusive cualquier procedimiento que requiera que un nacional de otra Parte señale un domicilio legal o designe un agente en el territorio de la Parte, si la excepción está permitida por la Convención pertinente listada en el Artículo 1701(2) y siempre que tal excepción:
a) Sea necesaria para asegurar el cumplimiento de medidas que no sean incompatibles con este capítulo; y
b) No se aplique en forma tal que constituya una restricción encubierta al comercio

4. Ninguna de las Partes tendrá conforme a este artículo obligación alguna relacionada con los procedimientos establecidos en acuerdos multilaterales concertados bajo los auspicios de la Organización Mundial de la Propiedad Intelectual en relación a la adquisición o conservación de derechos de propiedad intelectual.

Artículo 1705. Derechos de autor

1. Cada una de las Partes protegerá las obras comprendidas en el Artículo 2 del Convenio de Berna, incluyendo cualesquiera otras que incorporen una expresión original en el sentido que confiere a este término el mismo Convenio. En particular:

a) Todos los tipos de programas de cómputo son obras literarias en el sentido que confiere al término el Convenio de Berna y cada una de las Partes los protegerá como tales; y

b) Las compilaciones de datos o de otros materiales, legibles por medio de máquinas o en otra forma, que por razones de la selección o disposición de su contenido constituyan creaciones de carácter intelectual, estarán protegidas como tales.

La protección que proporcione una Parte conforme al inciso (b) no se extenderá a los datos o materiales en sí mismos, ni se otorgará en perjuicio de ningún derecho de autor que exista sobre tales datos o materiales.

2. Cada una de las Partes otorgará a los autores y a sus causahabientes los derechos que se enuncian en el Convenio de Berna respecto a las obras consideradas en el párrafo 1, incluyendo el derecho de autorizar o prohibir:

a) La importación a territorio de la Parte de copias de la obra hechas sin autorización del titular del derecho;

b) La primera distribución pública del original y de cada copia de la obra mediante venta, renta u otra manera;

c) La comunicación de la obra al público; y

d) La renta comercial del original o de una copia de un programa de cómputo

El inciso d) no se aplicará cuando la copia del programa de cómputo no constituya en sí misma un objeto esencial de la renta. Cada una de las Partes dispondrá que la introducción del original o de una copia del programa de cómputo en el mercado, con el consentimiento del titular del derecho, no agote el derecho de renta.

Cada una de las Partes dispondrá que para los derechos de autor y derechos conexos:

Cualquier persona que adquiera o detente derechos patrimoniales pueda, libremente y por separado, transferirlos mediante contrato para efectos de explotación y goce por el cesionario; y

b) Cualquier persona que adquiera o detente esos derechos patrimoniales en virtud de un contrato, incluidos los contratos de empleo que impliquen la creación de obras y fonogramas, tenga la capacidad de ejercitar esos derechos en nombre propio y de disfrutar plenamente los beneficios derivados de tales derechos.

4. Cada una de las Partes dispondrá que cuando el periodo de protección de una obra, que no sea fotográfica o de arte aplicado, deba calcularse sobre una base distinta a la de la vida de una persona física, el periodo no será menor de 50 años desde el final del año calendario en que se efectúe la primera publicación autorizada de la obra. A falta de tal publicación autorizada dentro de los 50 años siguientes a la realización de la obra, el período de protección será de 50 años contados desde el final del año calendario en que se haya realizado la obra

5. Cada una de las Partes circunscribirá las limitaciones o excepciones a los derechos que establece este artículo a casos especiales determinados que no impidan la explotación normal de la obra ni ocasionen perjuicio injustificadamente a los legítimos intereses del titular del derecho.

6. Ninguna de las Partes concederá licencias para la reproducción y traducción, permitidas conforme al Apéndice al Convenio de Berna, cuando las necesidades legítimas de copias o traducciones de la obra en el territorio de esa Parte pudieran cubrirse mediante acciones voluntarias del titular del derecho, de no ser por obstáculos creados por las medidas de la Parte.

En este apartado se establecen las obligaciones de los Estados parte en lo que se refiere a la regulación de la propiedad intelectual.

Así pues, se determina que la protección de los programas de cómputo serán de la misma forma como se protege a las obras literarias en el sentido como lo establece el Convenio de Berna para la protección de Obras Literarias y Artísticas de 1971, de igual forma las bases de datos serán determinadas y protegidas como

compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo. " [10]

Artículo 1711. Secretos industriales y de negocios

1. Cada una de las Partes proveerá a cualquier persona los medios legales para impedir que los secretos industriales y de negocios se revelen, adquieran o usen por otras personas sin el consentimiento de la persona que legalmente tenga bajo control la información, de manera contraria a las prácticas leales del comercio, en la medida en que: a) La información sea secreta, en el sentido de que, como conjunto o en la configuración y composición precisas de sus elementos, no sea conocida en general ni fácilmente accesible a las personas que normalmente manejan el tipo de información de que se trate;

b) La información tenga un valor comercial efectivo o potencial por ser secreta; y

c) En las circunstancias dadas, la persona que legalmente la tenga bajo control haya adoptado medidas razonables para mantenerla secreta.

2. Para otorgar la protección, cada una de las Partes podrá exigir que un secreto ndustrial o de negocios conste en documentos, medios electrónicos o magnéticos, liscos ópticos, microfilmes, películas u otros instrumentos similares.

. Ninguna de las Partes podrá limitar la duración de la protección para los secretos ıdustriales o de negocios, en tanto existan las condiciones descritas en el párrafo 1.

Ninguna de las Partes desalentará ni impedirá el licenciamiento voluntario de ecretos industriales o de negocios imponiendo condiciones excesivas o scriminatorias a tales licencias, ni condiciones que diluyan el valor de los secrètos dustriales o de negocios.

ɔmo lo establece el artículo anterior se determina sobre la provisión y los medios ɡales para impedir que los secretos industriales y de negocios, sean revelados,

---

onvenio de Berna para la Protección de Obras Literarias y Artísticas 1971

adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

En cuanto a lo que se refiere el párrafo 2, propone las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios. Y una de estás, es que dichos secretos consten en medios electrónicos o magnéticos.

Artículo 1714. Defensa de los derechos de propiedad intelectual

Disposiciones generales

1. Cada una de las Partes garantizará, conforme a lo previsto en este artículo y en los Artículos 1715 a 1718, que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual, que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en este capítulo, incluyendo recursos expeditos para prevenir las infracciones y recursos que desalienten futuras infracciones. Estos procedimientos se aplicarán de tal manera que se evite la creación de barreras al comercio legítimo y que se proporcione salvaguardas contra el abuso de los procedimientos.

2. Cada una de las Partes garantizará que sus procedimientos para la defensa de los derechos de propiedad intelectual sean justos y equitativos, que no sean innecesariamente complicados o costosos y que no impliquen plazos irrazonables o demoras injustificadas.

3. Cada una de las Partes dispondrá que las resoluciones sobre el fondo de un asunto en procedimientos administrativos y judiciales para la defensa de los derechos de propiedad intelectual deban:

(a) Preferentemente, formularse por escrito y contener las razones en que se fundan;

(b) Ponerse a disposición, cuando menos, de las partes en un procedimiento, sin demoras indebidas; y

(c) Fundarse únicamente en las pruebas respecto de las cuales se haya dado a tales partes la oportunidad de ser oídas.

4. Cada una de las Partes garantizará que las partes en un procedimiento tengan la oportunidad de obtener la revisión, por una autoridad judicial de esa Parte, de las resoluciones administrativas definitivas y, conforme a lo que señalen las disposiciones de las leyes internas en materia de competencia respecto a la importancia de un asunto, de obtener por lo menos la revisión de los aspectos jurídicos de las resoluciones judiciales de primera instancia sobre el fondo de un asunto. No obstante lo anterior, ninguna Parte estará obligada a otorgar la oportunidad de revisión judicial de las sentencias absolutorias en asuntos penales.

5. Nada de lo dispuesto en este artículo o en los Artículos 1715 a 1718 se interpretará en el sentido de obligar a cualquiera de las Partes a establecer un sistema judicial específico para la defensa de los derechos de propiedad intelectual distinto del sistema de esa Parte para la aplicación de las leyes en general.

6. Para efectos de lo previsto en los Artículos 1715 a 1718, el término "titular del derecho" incluirá a las federaciones y asociaciones que estén facultadas legalmente para ejercer tales derechos.

Respecto a este artículo los Estados partes señalan la defensa de los derechos de propiedad intelectual, a modo de que su derecho interno contenga procedimientos de defensa, que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual, comprendidos en el presente tratado.

rtículo 1717. Procedimientos y sanciones penales

. Cada una de las Partes dispondrá procedimientos y sanciones penales que se oliquen cuando menos en los casos de falsificación dolosa de marcas o de piratería e derechos de autor a escala comercial. Cada una de las Partes dispondrá que las anciones aplicables incluyan pena de prisión o multas, o ambas, que sean ficientes como medio de disuasión y compatibles con el nivel de las sanciones licadas a delitos de gravedad equiparable

2. Cada una de las Partes dispondrá que cuando corresponda, sus autoridades judiciales puedan ordenar el secuestro, el decomiso y la destrucción de las mercancías infractoras y de cualquiera de los materiales e instrumentos cuya utilización predominante haya sido para la comisión del ilícito.

3. Cada una de las Partes podrá prever la aplicación de procedimientos y sanciones penales en casos de infracción de derechos de propiedad intelectual, distintos de aquéllos del párrafo 1, cuando se cometan con dolo y a escala comercial.

Artículo 1718. Defensa de los derechos de propiedad intelectual en la frontera

1. Cada una de las Partes adoptará, de conformidad con este artículo, los procedimientos que permitan al titular de un derecho que tenga motivos válidos para sospechar que puede producirse la importación de mercancías falsificadas o pirateadas relacionadas con una marca o derecho de autor, presentar una solicitud por escrito ante las autoridades competentes, sean administrativas o judiciales, para que la autoridad aduanera suspenda su despacho para su libre circulación. Ninguna Parte estará obligada a aplicar tales procedimientos a las mercancías en tránsito. Cada una de las Partes podrá autorizar la presentación de una solicitud de esta naturaleza respecto de las mercancías que impliquen otras infracciones de derechos de propiedad intelectual, siempre que se cumplan los requisitos de este artículo Cada una de las Partes podrá establecer también procedimientos análogos relativos a la suspensión, por las autoridades aduaneras, de la liberación de las mercancías destinadas a la exportación desde su territorio.

2. Cada una de las Partes exigirá a cualquier solicitante que inicie un procedimiento de conformidad con el párrafo 1, que presente pruebas adecuadas:

a) Para que las autoridades competentes de esa Parte se cercioren de que, conforme a la legislación interna del país de importación, puede presumirse una infracción de su derecho de propiedad intelectual; y

b) Para brindar una descripción suficientemente detallada de las mercancías que las haga fácilmente reconocibles por las autoridades aduaneras.

Las autoridades competentes informarán al solicitante, en un plazo razonable, si han aceptado la solicitud y, cuando así ocurra, el periodo durante el cual actuarán las autoridades aduaneras.

3. Cada una de las Partes dispondrá que sus autoridades competentes tengan la facultad para exigir a un solicitante conforme al párrafo 1, que aporte fianza o garantía equivalente que sea suficiente para proteger al demandado y a las autoridades competentes, y para impedir abusos. Dicha fianza o garantía equivalente no deberá disuadir, de manera indebida, el recurso a estos procedimientos.

4. Cada una de las Partes dispondrá que, cuando en atención a una solicitud conforme a los procedimientos de este artículo las autoridades aduaneras hayan suspendido el despacho de las mercancías que conlleven diseños industriales, patentes, circuitos integrados o secretos industriales o de negocios, con fundamento en una resolución que no sea dictada por una autoridad judicial o por otra autoridad independiente, y el plazo estipulado en los párrafos 6 a 8 haya vencido sin que la autoridad debidamente facultada al efecto hubiere dictado una medida de suspensión provisional, y dado que se hubiera cumplido con todas las demás condiciones para la importación, el propietario, el importador o el consignatario de tales mercancías esté facultado para obtener la liberación de las mismas, previo depósito de una fianza por un importe suficiente para proteger al titular del derecho contra cualquier infracción. El pago de tal fianza no será en perjuicio de cualquier otro recurso que esté a disposición del titular del derecho, y se entenderá que la fianza se devolverá si el titular del derecho no ejerce su acción en un plazo razonable.

5. Cada una de las Partes dispondrá que su autoridad aduanera notifique con prontitud al importador y al solicitante sobre la suspensión de la liberación de las mercancías, de conformidad con el párrafo 1.

6. Cada una de las Partes dispondrá que su autoridad aduanera libere los bienes de la suspensión si en un plazo que no exceda a diez días hábiles, contados a partir de

que se haya notificado la suspensión al solicitante de conformidad con el párrafo 1, las autoridades aduaneras no han sido informadas de que:

a) Una parte que no sea el demandado ha iniciado el procedimiento conducente a una resolución sobre el fondo del asunto; o
b) La autoridad competente facultada al efecto ha adoptado medidas precautorias que prorrogan la suspensión, siempre que se hayan cumplido todas las demás condiciones para la importación o exportación Cada una de las Partes dispondrá que, en los casos apropiados, las autoridades aduaneras puedan prorrogar la suspensión por otros diez días hábiles.

7. Cada una de las Partes dispondrá que, si se han iniciado procedimientos conducentes a una resolución sobre el fondo del asunto, a petición del demandado se efectúe una revisión, otorgando derecho de audiencia, con el objeto de resolver en un plazo razonable si la aplicación de estas medidas será objeto de modificación, revocación o confirmación.

8. Sin perjuicio de lo dispuesto por los párrafos 6 y 7, cuando la suspensión de la liberación de las mercancías se efectúe o se continúe de conformidad con una medida judicial precautoria, se aplicará el Artículo 1716, 6).

9 Cada una de las Partes dispondrá que sus autoridades competentes tengan la facultad para ordenar al solicitante, de conformidad con el párrafo 1, que pague al importador, al consignatario y al propietario de las mercancías una indemnización adecuada por cualquier daño que hayan sufrido a causa de la retención indebida de las mercancías o por la retención de las mercancías que se hayan liberado de conformidad con lo dispuesto en el párrafo 6.

10. Sin perjuicio de la protección a la información confidencial, cada una de las Partes dispondrá que sus autoridades competentes tengan facultades para conceder al titular del derecho oportunidad suficiente para hacer inspeccionar cualquier

mercancía retenida por las autoridades aduaneras, con el fin de sustanciar las reclamaciones del titular del derecho. Cada una de las Partes dispondrá también que sus autoridades competentes tengan la facultad para conceder al importador una oportunidad equivalente de hacer inspeccionar esas mercancías Cuando las autoridades competentes hayan dictado una resolución favorable sobre el fondo del asunto, cada una de las Partes podrá conferirles la facultad para informar al titular del derecho acerca de los nombres y domicilios del consignador, del importador y del consignatario, así como la cantidad de las mercancías en cuestión.

11. Cuando una Parte requiera a sus autoridades competentes actuar de oficio y suspender la liberación de mercancías respecto de las cuales tengan pruebas que a primera vista hagan presumir que se está infringiendo un derecho de propiedad intelectual.

a) Las autoridades competentes podrán requerir, en cualquier momento, al titular del derecho cualquier información que pueda auxiliarles en el ejercicio de estas facultades;

b) El importador y el titular del derecho serán notificados con prontitud acerca de la suspensión por las autoridades competentes de la Parte, y cuando el importador haya solicitado una reconsideración de la suspensión ante las autoridades competentes, ésta estará sujeta, con las modificaciones necesarias, a las condiciones establecidas en los párrafos 6 a 8; y

c) La Parte eximirá únicamente a las autoridades y funcionarios públicos de la responsabilidad a que den lugar las medidas correctivas adecuadas tratándose de actos ejecutados o dispuestos de buena fe.

12. Sin perjuicio de las demás acciones que correspondan al titular del derecho y a reserva del derecho del demandado de solicitar una revisión ante una autoridad judicial, cada una de las Partes dispondrá que sus autoridades competentes tengan la facultad para ordenar la destrucción o eliminación de las mercancías infractoras de conformidad con los principios establecidos en el Artículo 1715, 5). En cuanto a las mercancías falsificadas, las autoridades no permitirán, salvo en circunstancias

excepcionales, que se reexporten en el mismo estado, ni las someterán a un procedimiento aduanero distinto.

13. Cada una de las Partes podrá excluir de la aplicación de los párrafos 1 a 12, las cantidades pequeñas de mercancías que no tengan carácter comercial y formen parte del equipaje personal de los viajeros o se envíen en pequeñas partidas no reiteradas

14 El Anexo 1718.14 se aplica a las Partes señaladas en ese anexo

Anexo 1718.14

Defensa de los derechos de propiedad intelectual

México hará su mayor esfuerzo por cumplir tan pronto como sea posible con las obligaciones del Artículo 1718, y lo hará en un plazo que no exceda tres años a partir de la fecha de firma de este Tratado.

Artículo 1719. Cooperación y asistencia técnica

1. Las Partes se otorgarán mutuamente asistencia técnica en los términos que convengan y promoverán la cooperación entre sus autoridades competentes. Dicha cooperación incluirá la
capacitación de personal.

2. Las Partes cooperarán con miras a eliminar el comercio de productos que infrinjan los derechos de propiedad intelectual. Con tal fin, cada una de ellas establecerá y dará a conocer a las otras Partes al 1o. de enero de 1994, los puntos de enlace en sus gobiernos federales, e intercambiará información relativa al comercio de mercancías infractoras.

En el presente ordenamiento se comprende los procedimientos y sanciones penales que cada parte debe manejar en su derecho, asimismo se contemplan las figuras como la piratería de derechos de autor a escala comercial.

cuanto a las obligaciones relativas a la defensa de los derechos de propiedad ectual frontera, que el artículo 1718 establece, México se compromete a realizar mayor esfuerzo por cumplir tan pronto como le fuere posible, dichas gaciones. Por lo que en el anexo 1718.14 se establece un plazo que no excederá es años a partir de la fecha de la firma del Tratado de Libre Comercio en Norte érica para cumplir con tales obligaciones.

o que se refiere al artículo 1719, relativo a la cooperación y asistencia técnica, las es, señala, se otorgarán mutuamente asistencia técnica en los términos que vengan y promoverán la cooperación entre sus autoridades competentes. Dicha peración incluirá la
acitación de personal. Cooperación con miras a eliminar el comercio de productos infrinjan los derechos de propiedad intelectual.

esta manera podemos ubicar el punto de vista de este tratado en su Sexta Parte, ítulo XVIII, disposición que se encuentra regulando estos programas de nputo.

CAPITULO IV ESTUDIO ANALITICO Y COMPARATIVO ENTRE LA LEGISLACIÓN NACIONAL Y OTRAS LEGISLACIONES INTERNACIONALES

4.1 Otras legislaciones internacionales como lo son Argentina, Alemania, Austria, Francia, Chile, Gran Bretaña, Holanda, Estados Unidos y España.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios Las más diversas esferas del conocimiento humano, en lo científico. en lo técnico. en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimientos puede obtenerse, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía,

configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

De esto se desprende que el creciente aumento de las conductas delictivas tendientes a destruir, modificar, piratear o incluso sabotear información confidencial de Instituciones internacionales con una seguridad impresionante, obligo en un principio a los países desarrollados regular dichos delitos, con la finalidad de salvaguardar la seguridad de su información y su intimidad profesional, federal o inclusive personal

Con el objeto de realizar un estudio analítico y comparativo entre nuestra legislación nacional y la legislación internacional, se presentará los casos particulares de algunos países desarrollados y subdesarrollados que se han preocupado por disponer una legislación adecuada para regular la problemática que existe en el ámbito de la informática. Así en los puntos subsecuentes a desarrollar en el presente capítulo podremos analizar y observar cuales son las medidas de seguridad que se podrán implantar dentro de la legislación nacional

Argentina

En la Argentina, aún no existe legislación especifica sobre los llamados delitos informáticos.
Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11 723 de propiedad intelectual gracias al Decreto Nº 165/94 del 8 de febrero de 1994

En dicho Decreto se definen:
Obras de software: Las producciones que se ajusten a las siguientes definiciones:
1. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.

2.Los programas de computadoras. tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por la computadora.

3.La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

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

De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa, entendiendo como cosas aquellos objetos materiales susceptibles de tener algún valor, la energía y las fuerzas naturales susceptibles de apropiación. (Código Civil, Art. 2311).

Asimismo, la situación legal ante daños infligidos a la información es problemática.
El artículo 1072 del Código Civil argentino declara "el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama. en este Código, delito", obligando a reparar los daños causados por tales delitos.

En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, "la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo" (Art. 1094).

Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que "alguien por su culpa o negligencia ocasiona un daño a otro" (Art. 1109).

Alemania

En Alemania, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986,en la que se contemplan los siguientes delitos:

- Artículo 202 a. Espionaje de datos
- Artículo 263 a. Estafa informática

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

- Artículo 269. Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(artículos 270, 271, 273)
- Artículo 303 a. Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Artículo 303 b. Sabotaje informático destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Artículo 266 b. Utilización abusiva de cheques o tarjetas de crédito

Sobre el particular se entiende que el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, este no sólo ha renunciado a tipificar la mera

penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

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

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos
Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

Austria

Ley de reforma del Código Penal de el 22 de diciembre de 1987.
Esta ley contempla los siguientes delitos:
- Artículo 126. Destrucción de datos En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Artículo 148. Estafa informática. En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del

procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

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

- Artículo 462-2. Acceso fraudulento a un sistema de elaboración de datos. En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Artículo 462-3 Sabotaje informático. En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Artículo 462-4 Destrucción de datos. En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Artículo 462-5. Falsificación de documentos informatizados. En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Artículo 462-6. Uso de documentos informatizados falsos. En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Chile.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus

Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

Gran Bretaña

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

Holanda.

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Estados Unidos

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

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

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

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

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

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

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

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

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

España.

En el Nuevo Código Penal de España, el art 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intensión dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

4.2 Lagunas dentro de la legislación mexicana.

La problemática que se ha venido suscitando a través de los tan comentados delitos informáticos dentro de los sistemas computacionales, ha generado como lo comentaba en el punto anterior del presente trabajo, un desastre internacional que en ocasiones a traído consigo consecuencias catastróficas implicando la seguridad internacional. Es por ello que nuestros legisladores se han concientizado al respecto, consagrando ordenamientos básicos con la intención de regular dichos delitos. Estas conductas delictivas se encuentran reguladas en el Código Penal Federal y en la Ley Federal de Derechos de Autor, ordenamientos que contienen lagunas con relación a la materia de la informática, ya que como hemos venido mencionando no protegen aspectos de suma importancia como lo es la intimidad, seguridad patrimonial, dignidad e inclusive daños morales.

Código Penal Federal.

Dentro del Código Penal Federal nos hemos podido percatar de las innumerables reformas, adiciones y derogaciones que el mismo ha venido sufriendo a través de la historia penal mexicana. Aunque varias de estas reformas han traído una mejoría a nuestro sistema legal, otras tantas solo han sido adiciones que han demostrado que el aumento de penas no ha servido como una forma de disuasión, puesto que en nuestro Código Penal vemos el aumento de penas, como ya lo hemos mencionado. pero la delincuencia sigue creciendo a pasos agigantados.

Para disuadir la comisión de delitos, lo eficaz es que no exista impunidad. Que encontremos en agentes del Ministerio Público, Jueces. Magistrados y Ministros. una labor eficiente en la procuración y administración de justicia para que se sancione a los responsables de los delitos.

Es por ello que es indispensable y urgente el crear medidas de prevención, por lo que invariablemente surgen las siguientes preguntas, ¿de que sirve tener penas de cincuenta años o más, si las personas acusadas de los delitos que tienen tales sanciones son absueltos por intereses particulares? o ¿de que sirve tener a la mayoría de estos delincuentes en prisión, cuando la totalidad de nuestros centros de readaptación social (llamados también reclusorios), están saturados o sobre poblados?. Creando así pues de estos centros una escuela de criminales profesionales. de tal forma que no se cumple con su objetivo, que es el de readaptar a dichos criminales, para el bienestar social.

Así pues, es como nos encontramos (la sociedad en su totalidad), en la tarea de buscar y encontrar una forma o medida de prevenir los delitos informáticos, que como hemos venido señalando a lo largo de este trabajo de investigación. a causado innumerables esfuerzos (por parte de la comunidad internacional) para definir, tipificar y sancionar dichos delitos.

De tal manera y conforme a lo establecido en este numeral se señalarán las lagunas existentes dentro del Código Penal Federal, enfocadas a los " Delitos Informáticos ", con el fin de analizarlos. para dejar en claro el motivo indispensable de crear una ley que regule, tipifique y sancione dichos delitos como tales.

Durante las reformas realizadas al Código Penal Federal, en relación al Título Noveno que el 17 de mayo de 1999 se público en el Diario Oficial, se puede observar en forma considerada la ausencia de la Comisión de Ciencia y Tecnología. así como de representantes expertos en el área de la informática. en los procesos de presentación, discusión y elaboración de esta reforma. Participación que además de armonizar su contenido con las demandas e inquietudes legales de los principales usufructuarios del multimedia, sin lugar a dudas habría dotado a este ordenamiento de un importante matiz neojurídico - tecnológico, y por supuesto de la imprescindible especialización, representatividad y legitimidad sectorial que en nuestros tiempos requiere la labor legislativa.

Podemos observar la desproporción e inequidad existente entre las penalidades y sanciones pecuniarias enumeradas por esta norma, para sancionar íntima y selectivamente las diferentes modalidades o hipótesis materiales, por lo que en estricto apego a la ley debería de ser un mismo delito. Asimismo se han establecido criterios discriminatorios determinados arbitrariamente en atención a la calidad de las personas físicas y morales, o bien, de las entidades públicas que hayan sido víctimas de los infractores cibernéticos. Sin lugar a duda, lo anterior demuestra una vez más el imperio supra constitucional del Estado mexicano y sus instituciones sobre el resto de las organizaciones sociales y mercantiles del país, aún por encima de aquellas que por su naturaleza guardan en sus sistemas computacionales importantes diseños industriales e información comercial de incuantificable valor estratégico y económico. No podemos explicarnos de otra manera la disparidad existente entre las sanciones establecidas por el reformulado Código Penal para este tipo de ilícitos.

En cuanto a los artículos 424 al 429 de este ordenamiento, que pertenecen por su naturaleza a la materia de derechos de autor, regulan también las conductas realizadas por los llamados " Delitos Informáticos " (llamados así en las legislaciones internacionales), observando así pues que el bien jurídico a tutelar es la propiedad intelectual lo que de esta manera se limita su aplicación de manera considerable. Ya que si nos ponemos a analizar concretamente los " Delitos Informáticos " tienen también otros bienes jurídicos a tutelar como lo son la intimidad, la seguridad patrimonial, la dignidad y los daños morales ocasionados, mismos que aún no han podido protegerse en este ordenamiento.

Ley Federal del Derecho de Autor

En cuanto a la Ley Federal del Derecho de Autor , podemos referirnos que en su artículo 109 se establece la protección de las bases de datos personales, protección sin duda alguna necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política.
Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero.

De esta forma el análisis de este artículo confirma la ubicación que hemos sostenido respecto a que en las conductas ilícitas relacionadas con la informática el bien jurídico a tutelar no es únicamente la propiedad intelectual sino entre otros también se encuentra la protección de la intimidad personal, la seguridad patrimonial, la dignidad y los daños morales ocasionados, por lo que este artículo no debería formar parte de una Ley Federal de Derechos de Autor sino de una legislación especial tal y como se ha hecho en otros países.

En lo que respecta al artículo 231, fracciones II y VII se contemplan las infracciones de comercio como son las de producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por la Ley Federal del Derecho de

Autor y usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular.

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

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

4.3 La necesidad de la creación de una ley que regule y sancione los delitos informáticos.

Según el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la Organización de las Naciones Unidas resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a. Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

b. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

c. Falta de especialización de las policías fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

d. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

e. Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

Respecto al inciso b, que se resume en la ausencia de acuerdos globales en la definición legal de dichas conductas delictivas, encontramos que existe la falta de un consenso sobre la definición jurídica clara y precisa, de los delitos informáticos, así como de la falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, por lo que trae aparejada indudablemente las dificultades de carácter procesal y la ausencia de una investigación.

De esta manera la ausencia de la especialización en el campo de los delitos informáticos, por parte de las autoridades judiciales y legislativas, tal y como lo señala el inciso c, crean una insuficiente, enorme y clara realidad legislativa, ya que gracias a esta ausencia dicha legislación encuentra en su práctica una pobre realidad.

Tal como lo señala el inciso d la falta de armonización que existe entre las diferentes leyes procesales nacionales, acerca de la investigación de los delitos informáticos, podemos observar que nuestra legislación mexicana se encuentra en esta problemática, ya que a pesar de existir ordenamientos legales que " regulen las conductas realizadas por los llamados " Delitos Informáticos " (llamados así en las legislaciones internacionales), es insuficiente su labor y su penalización, por que aunque el Título Vigésimo Sexto del Código Penal Federal, hace referencia de la

aplicación de una sanción con una multa de trescientos a tres mil días o pena de prisión de seis meses hasta seis años, al que incurra en este tipo de delitos, o inclusive en el Titulo Noveno de dicho ordenamiento, señala de igual forma la pena de prisión de dos hasta ocho años, y de trescientos a novecientos días multa, al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, dichas referencias existentes en la regulación mexicana, no han llegado a contemplar al delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial. así como también se establecieron criterios discriminatorios determinados arbitrariamente en atención a la calidad de las personas físicas y morales, o bien, de las entidades públicas que hayan sido víctimas de los infractores cibernéticos, de igual forma la desproporción e inequidad existente entre las penalidades y sanciones pecuniarias enumeradas por esta norma, son más que evidentes.

En otro orden de ideas por ejemplo en el artículo 109 de la Ley Federal de Derecho de Autor, hace una cita de la regulación en cuanto a la protección de las bases de datos personales, es decir, este ordenamiento " regula precariamente la protección de la intimidad ", que en opinión de otras legislaciones a nivel internacional (como lo he señalado en el primer apartado del presente capítulo) es indispensable proteger, debido a que como se ha venido explicando con anterioridad que el bien jurídico a tutelar en los delitos informáticos, no es únicamente la propiedad intelectual, sino también se encuentra la intimidad personal, la seguridad patrimonial, la dignidad e inclusive los daños morales.

El Derecho a la intimidad o privacía es un Derecho Fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que puede ser develado por existir un derecho superior de terceros o para el bienestar común. Por lo que se debe de asistir a la garantía de legalidad en cuanto a

lo que respecta a reparar las posibles molestias a la persona o propiedades y posesiones, conforme al las normas constitucionales, que regulan los derechos fundamentales.

Así pues, podemos observar que en el artículo 16 Constitucional, se encuentra regulada la garantía de seguridad jurídica. que en su primera parte a la letra dice:
" Nadie puede ser molestado en su persona, familia. domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente. que funde y motive la causa legal del procedimiento "
Es, sin duda alguna un ordenamiento amplio y suficiente que garantiza el derecho a la privacidad. a la intimidad de los individuos, pues regula con precisión los requisitos que debe reunir el mandamiento legal escrito, mediante el cual pueda afectarse a molestarse a la persona con utilización de algún medio.

El primer texto constitucional en Europa que recogió de forma expresa el derecho a la intimidad fue la Constitución portuguesa de 1986, según se menciona en el artículo 35 que explica

" 1 -Todos los ciudadanos tendrán derecho a informarse del contenido de bancos de datos acerca de ellos y de la finalidad a que se destinen las informaciones y podrán exigir la rectificación de los datos, así como su actualización.
2.-Los terceros tendrán prohibido el acceso a archivos con datos personales y a las intercomunicaciones que surjan de ellos así como a los flujos de información transnacionales, salvo en casos excepcionales previstos por la ley
3 -No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.
4.-La ley determinará el concepto de datos personales para el propósito de bancos de datos.
5 -Los ciudadanos no podrán recibir un número de identificación único usable para todo tipo de propósitos. "

Existe la elaboración doctrinal que sirve de precedente para el derecho a la intimidad concebido como "The rigth to be let alone" (el derecho a ser dejado solo, a ser dejado en paz), por el Juez Cooley, documento que se originó en 1890, a propósito de un amplio artículo publicado por los abogados Samuel D. Warren y Louis D. Brandeis, en la Harvard Review titulado "The Right to Privacy". Este artículo contiene las bases doctrinales a partir de las cuales se han desarrollado el derecho a la intimidad.

De acuerdo al análisis anterior y conforme a todos estos ordenamientos, fuentes doctrinales y principios mencionados, se puede deducir finalmente la necesidad de la creación de una ley especial que regule y proteja estos bienes jurídicos a tutelar como lo son la intimidad personal, la seguridad patrimonial, la dignidad y los daños morales ocasionados, tanto al particular como al estado; derechos que se han visto violados, agredidos y ofendidos en distintas circunstancias por la realización de dichos delitos informáticos.

Así como también deberá explicar y especificar dicha Ley, la autoridad ante la cual se va a dirigir el ofendido y el ordenamiento que se deberá seguir para poder llevar a cabo el procedimiento legal, o sí en su defecto por la naturaleza del delito requiere de un procedimiento especial.

Además de que deberán encontrarse tipificado los delitos informáticos en el Código Penal Federal, para que la ley tenga un soporte en dicho Código.

CONCLUSIONES

PRIMERA.- A lo largo de la historia del hombre se han obtenido tecnologías modernas que ponen en alerta al individuo para seguir adelante sin parar y lograr así la perfección, percatándonos entonces que el avance progresivo con el que se desarrolla la informática en el mundo del ciberespacio, a traído consigo enormes beneficios a la humanidad que facilitan en gran medida las tareas y actividades del ser humano arrastrando con ello desafortunadamente, conductas ilícitas que en determinadas ocasiones ponen en peligro la intimidad, el patrimonio e inclusive la propia vida de la persona.

SEGUNDA.- Quedando así establecido que dicho avance informático debe y tiene que regularse en cada país tomando en cuenta ante todo los tratados internacionales, acuerdos y convenios realizados entre estos, para así poder obtener una cooperación y un resultado eficaz por parte de dichos países una vez instituidas sus legislaciones, y así poder combatir determinantemente las conductas ilícitas realizadas por los delitos informáticos.

TERCERA.- En la actualidad en nuestro sistema legal, no existe un concepto de delito informático, por lo que es importante que se realice no sólo para conocer las limitantes de éste, sino también para lograr que se tipifique este delito como tal en el Código Penal Federal vigente, y así poder sancionarlo y regularlo

CUARTA.- Es interesante e indispensable conocer los tipos del delito informático, que señala la ONU (Fraudes cometidos mediante manipulación de computadoras. Entre este tipo se encuentran la Manipulación de los datos de entrada, la manipulación de los datos de salida; Falsificaciones informáticas como objeto y como instrumentos; Acceso no autorizado a servicios y sistemas informáticos; Piratas informáticos o Hackers; La Reproducción no autorizada de programas informáticos de protección legal y Daños o modificaciones de programas o datos computarizados

como lo es el sabotaje informático a través de los virus, gusanos y la bomba lógica), antes que nada para poder tener en claro las consecuencias que se producen con la realización de estas conductas ilícitas y sobre todo por que con esta referencia se podrá prevenir firmemente dichas consecuencias.

QUINTA.- Se ha dejado en claro que la celeridad y la ligereza con las que se realizaron las reformas al Código Penal Federal en materia de Derechos de Autor y de Sistemas de Cómputo, dejaron dudas por resolver como por ejemplo: ¿ ante que *autoridad con conocimientos en informática deberá presentarse la víctima* de estas conductas ilícitas ? o ¿ en que parte del Código Penal Federal se encuentra tipificado el Delito Informático como tal ? o ¿ que procedimiento se deberá seguir para sancionar este tipo de delitos, o es acaso que se tendrá que seguir el procedimiento penal con la ausencia implícita de un representante experto en la materia de la informática ?.

SEXTA.- Si bien se entiende que la Ley Federal del Derecho de Autor hace una remisión al Código Penal Federal, para que tenga conocimiento de las conductas especificadas en la Ley Federal del Derecho de Autor y que además no sólo las tenga contempladas sino que señale a parte multas. Es también muy cierto que aunque se presenten estas multas, no se encuentra tipificado el delito como tal. y sólo se multan ciertas conductas dejando a la deriva impunemente muchas otras conductas ilícitas que requieren necesariamente pagar un castigo por los daños causados, que en muchas de las ocasiones no se pueden restituir.

SIETE.- Con todo lo anterior se propone se realice la creación de una ley que regule y sancione los delitos informáticos, protegiendo los bienes jurídicos a tutelar como lo son la intimidad personal, la seguridad patrimonial y la dignidad, estableciendo un procedimiento especial a seguir dada la naturaleza del mismo. Además de que estos delitos deberán encontrarse tipificados en el Código Penal Federal.

BIBLIOGRAFÍA DE TESIS

ALTMARK, Daniel Ricardo. Informática y Derecho. Editorial Depalma. Buenos Aires. 1996.

ALVÁREZ, Mario I. Introducción al Estudio del Derecho. De. Mc Graw Hill. México.1995.

BARRAGAN, Julia. Informática y Decisión Jurídica. Editorial Fontamora. México.1994.

C. MEJÁN, Luis Manuel. El derecho a la intimidad. Editorial Porrúa. México. 1996.

CARRANCÁ y Trujillo, Raúl. Derecho Penal Mexicano. Editorial Porrúa. México. 1996.

CASTELLANOS Tena, Fernando. Lineamientos Elementales de Derecho Penal. Editorial Porrúa. México. 1997.

DAVARA Rodríguez, Miguel Angel. Derecho Informático. Editorial Aranzadi. Pamplona, España. 1993.

FIX Fierro, Héctor. Informática y Documentación Jurídica. UNAM Facultad de Derecho. México. 1997.

GIRALDO, Angel. Informática Jurídica Documental. Editorial Temis. Bogotá, Colombia. 1996.

LÓPEZ Betancourt, Eduardo. Delitos en Particular. Editorial Porrúa. México. 1998.

LÓPEZ Betancourt, Eduardo. Introducción al Derecho Penal. Editorial Porrúa. México. 1998.

M. FALCON, Enrique. ¿ Qué es la informática Jurídica ?. Editorial Abeledo-Perrot. Buenos Aires. 1995.

MOLINA Mateos, José María. Seguridad, información y poder. Editorial INCIPIT. Madrid, España. 1994.

PÉREZ Luño, Antonio Enrique. Ensayos de Informática Jurídica. Editorial Fontamora. México. 1996.

PRADO, Pedro Antonio. La Informática y el Abogado. Editorial Abeledo-Perrot. Buenos Aires. 1988.

TELLEZ Valdés, Julio. Derecho Informático. Editorial Mc Graw Hill. México. 1996.

L E Y E S

Constitución Política de los Estados Unidos Mexicanos. Editorial Porrúa.1999

Código Penal Federal. Editorial Porrúa. 2000

Legislación sobre Propiedad Industrial e Inversiones Extranjeras. Colección Porrúa. Editorial Porrúa. 1997.

Ley Federal del Derecho del Autor. Editorial Porrúa. México. 1999.

Tratado de Libre Comercio de América del Norte (TLC), Sexta parte, Capítulo XVII, Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.