294

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS COMO DELITO EN EL DISTRITO FEDERAL. ALGUNAS CONSIDERACIONES LEGALES.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

DAVID ROBERTO MERCADO ROJAS

ASESOR: LIC. ENRIQUE M. CABRERA CORTES

MÉXICO, D.F. 2002

Hay una mujer que, siendo joven, tiene la reflexión de una anciana y en la vejez trabaja con el vigor de la juventud. Una mujer que, si es ignorante, descubre los secretos de la vida con más acierto que un sabio y, si es instruida, se acomoda a la sencillez de los niños.
Es quien siendo pobre satisface con la felicidad de los que ama y, siendo rica, daría con gusto sus tesoros por no sufrir en su corazón la herida de la ingratitud.
Esa mujer que, mientras vive, pocas veces sabemos apreciar por que a su lado todos los dolores se olvidan. Sin embargo, después de muerta, daríamos todo lo que somos y todo lo que tenemos por mirarla de nuevo un solo instante, por recibir un solo abrazo, por escuchar una sola palabra... de los labios de nuestra madre.

Te amo mamá.

DEDICATORIAS

En principio este espacio lo había pensado llenar con una lista de dedicatorias de las personas que en mi opinión eran las indicadas para estar aquí, pero Dios me arrebato en un abrir y cerrar de ojos a mi Madre; es algo indescriptible, no me puedo imaginar que ella no estará más a mi lado, que ya no me contestará el teléfono cuando llame a casa; que ya no podré compartir con ella el desayuno, comida o cena, saber que físicamente no estará conmigo al presentar mi examen profesional y en ningún otro momento. Por eso es que dedico este espacio a la mujer que me dio el mejor regalo: "la vida", a la mujer que siempre fue mi amiga, a la mujer que me brindó su apoyo incondicional por sobre todas las cosas, y que nunca podré pagarle lo que hizo por mí; por eso es que este trabajo y todos mis triunfos se los dedico a la mujer que más he amado en mi vida:

A MI MADRE (ESTELA ROJAS VILLALOBOS - q.e.p.d.-), por que se, que aun desde el cielo estarás conmigo. TE AMO.

AGRADECIMIENTOS

GRACIAS:

A Dios:
Por darme la fortaleza y serenidad de seguir adelante.

A mi madre. (q.e.p.d.)
Por haberme forjado como persona; por que sin su impulso este trabajo no tendría vida y por que simplemente sin ella, yo no existiría.
Gracias mamá, donde quiera que estés.

A mi padre:
David Jorge Mercado Limón, por la fe y esperanza que tiene en mi, así como por sus consejos, sus enseñanzas y por ser un ejemplo en mi vida. Gracias Papá. Te quiero.

A mis hermanos:
Martín, Jorge y Estela, por compartir conmigo los mejores y peores momentos en mi vida, por su amor y apoyo y, por que gracias a su impulso he podido salir adelante. Gracias, los quiero mucho.

A toda mi familia (Abuelos, Tías, primos, sobrinos y cuñadas)
Por todo su cariño y apoyo. Gracias.

A mi novia:
Yolanda Gómez Muñoz, por brindarme tu amor, tu apoyo, tu compresión, y una parte de tu vida.
Gracias mi amor.

A todos mis amigos:
Por que han estado en los momentos que más los he necesitado y por que más que amigos los considero mis hermanos. Gracias pránganas.

A mis compañeros de trabajo:
Por su solidaridad mostrada en todo momento.

A mi amiga Angélica Blanco:
Por todo su apoyo y sobre todo por la amistad incondicional que me ha brindado. Gracias.

A mi compañera y amiga:
Yesenia Ramírez Velasco, por el impulso y apoyo brindado. Gracias.

A la Escuela Nacional de Estudios Profesionales Aragón, por brindarme la oportunidad de forjarme como universitario y abrirme la puertas del conocimiento.

Al Licenciado Bruno Cruz Jiménez, Juez Vigésimo Primero de lo Civil en el D.F. por darme la oportunidad de forjarme como persona y como profesional y por ser uno de los mejores maestros que he tenido en mi carrera. Gracias.

A mi asesor el Lic. Enrique Cabrera Cortes, por que en el encontré mas que un asesor, encontré un amigo. Gracias.

ÍNDICE

CAPITULO 3.

LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICO COMO DELITO EN EL DISTRITO FEDERAL. ALGUNAS CONSIDERACIONES JURÍDICAS.

INTRODUCCIÓN.

La década de los noventas se caracterizó por el vertiginoso desarrollo de todo lo relativo a la informática, disciplina que pasó de ser un lujo o privilegio exclusivo de la clase media alta y alta, a convertirse en una herramienta imprescindible en la vida diaria de casi todas las personas. Con la aparición de Internet, nuestra vida experimentó otro notable cambio, puesto que en cuestión de segundos podemos acceder a lugares lejanos, sin importar distancias, horarios o diferencias sociales, políticas, religiosas o culturales.

Si bien es cierto, no podemos aseverar que en la actualidad todos los mexicanos posean una computadora (aunque sería ideal), lo cierto y real es que cada día más de la población mexicana entran al fascinante mundo de ellas. Tengamos en cuenta que últimamente han proliferado los llamados cafés Internet, donde se pueden rentar por hora computadoras y el uso o navegación de Internet, por un precio de cinco, diez o veinte pesos por hora.

Dentro de la informática, indudablemente que el Internet merece una mención especial. Red de redes, Internet es una gran interconexión de computadoras entre sí que se encuentran unidas a una computadora central para el intercambio de información, de bienes o servicios. Actualmente, Internet es una

gran ventana al mundo y el medio de comunicación masiva más rápido y barato que existe. Hoy, podemos hablar de una "comunicación virtual", de compras y ventas "virtuales" y en general, de un mundo "virtual", el cual se mueve y vive mediante las computadoras y en lo particular de Internet.

Uno de los principales problemas y preocupaciones es que Internet sigue careciendo de una adecuada regulación jurídica, por lo que continúa siendo una súper red anárquica, lo que no brinda mucha seguridad en las transacciones económicas y comerciales realizadas en la red. Esa anarquía ha sido bien aprovechada por personas sin escrúpulos quienes han operado desde el anonimato para robar información y obtener grandes beneficios económicos, pero también, han creado diversos programas computacionales destinados a causar el caos en las computadoras interconectadas, dañando sus programas y sus discos duros en el peor de los casos, lo que se traduce en menoscabos o detrimentos económicos o patrimoniales a los usuarios de la red. A estos programas se les ha dado el nombre de **"virus informáticos"**, por los efectos que causan al ser recibidos en una computadora y la facilidad con la que pueden ser propagados por los "hackers" o sujetos creadores y propagadores de ellos.

Finalmente, cabe destacar que en muchos países ya existe algún tipo especial que regula y sanciona a quienes se dedican a crear y propagar algún

tipo de virus informático, lo cual no sucede en algunas ciudades importantes, como por ejemplo, en el Distrito Federal de manera inexplicable. Agregaremos que si bien existe en materia Federal una simple regulación de los delitos informáticos, es evidente la carencia de un marco legal adecuado en nuestro país. En otras latitudes como España, Argentina, Alemania, etc. existe además de ese marco legal tan necesario, una policía cibernética o científica encargada de investigar los delitos informáticos.

En la presente investigación abordamos el estudio de la creación y la propagación de virus informáticos como una modalidad de los delitos informáticos, tema que parecería algo novedoso; sin embargo, no lo es tanto, puesto que la realidad es contundente al respecto.

La investigación está dividida en tres capítulos perfectamente delimitados. En el primero de ellos, abordamos el aspecto histórico de las computadoras; en el segundo, los aspectos más generales de las mismas y; en el tercero, la creación y propagación de virus informáticos como delito, donde hacemos algunas propuestas tanto legislativas como sociales que estimamos son de utilidad para enfrentar este tipo de conductas que causan serios daños patrimoniales a los usuarios de las computadoras.

CAPÍTULO 1.

ANTECEDENTES DE LAS COMPUTADORAS.

1.1. LA CREACIÓN DE LAS COMPUTADORAS.

Las computadoras constituyen uno de los inventos o creaciones más impresionantes y revolucionarias que ha podido cristalizar el hombre. Hace cuarenta o cincuenta años parecía un sueño que el hombre se auxiliara de una máquina o especie de robot para realizar sus trabajos estadísticos, organizativos o de investigación; sin embargo, gracias a algunos años de esfuerzos se pudo materializar ese sueño llamado: computadora. Actualmente no entenderíamos nuestro mundo globalizado sin la existencia de las computadoras las cuales se han ido perfeccionando y estilizando mucho hasta llegar a contar con aparatos sofisticados que se convirtieron rápidamente en oficinas móviles y en los mejores compañeros de trabajo.

Paulatinamente nace de esta manera una disciplina llamada "cibernética", cuya función es explicar las relaciones entre el hombre y las computadoras.

El término "cibernética" proviene de la voz griega "kybernetes", piloto, y de "kybernes", que se refiere al arte de gobernar.

El autor Julio Téllez Valdez dice que la cibernética es:

". . . . . la ciencia de la comunicación y el control. Los aspectos aplicados de esta ciencia están reclamados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, extractada de los campos de aplicación y adecuada para todos ellos"[1]

La cibernética es una ciencia multidisciplinaria que se relaciona con todas las ramas del conocimiento humano. Según relata el autor citado, en el año de 1948, un matemático de los Estados Unidos, Norbert Wiwnwe, escribió un libro llamado precisamente "cibernético", empleando quizá, por primera vez el término para designar una novel ciencia de la comunicación y el control entre el ser humano y las computadoras.

Dentro de las causas que originaron la aportación de la cibernética Téllez Valdez cita las siguientes:

"a) Un factor social, por que eran tiempos que requerían un aumento de la producción y por consiguiente, en el capital. Eran tiempos duros, sin embargo, se necesitaba más que una emergencia racional para que gestara una nueva creencia. Es así como Stanfford Beer en Cibernética y administración

[1] Téllez Valdez, Julio. Derecho Informático. Editorial Mc Graw Hill, 2ª edición, México, 1996, p. 4.

señaló que el clima intelectual debe ser tal que favorezca el surgimiento de una nueva disciplina.

b) El factor técnico-científico, fue muy importante por que varias líneas de pensamiento, originadas en muy diversas esferas de actividad, como lo fue la ciencia, se empezaron a reunir y lograron avances tales que hicieron menester una ciencia que facilitara su interrelación y desenvolvimiento.

c) Un tercer factor, el histórico, por que surge la mencionada necesidad del nacimiento de una ciencia de unión que controlara y vinculara a todas las demás. Surge entonces la cibernética como una unidad multidisciplinaria. . . ."[2]

Hoy la cibernética es toda una realidad y una ciencia multidisciplinaria que ha ayudado al avance o desarrollo de todo lo concerniente a las computadoras.

Los creadores de las computadoras han desarrollado en los últimos años variados programas o software que han venido a facilitar más las labores diarias de la gente, tales como son: Windows en sus diversas versiones, (95, 98, ME, XP), sin embargo, uno de los recursos que realmente ha revolucionado

[2] Ibid. p.3.

al mundo de las computadoras es el Internet que es en términos generales una súper carretera de información, donde se interconectan las computadoras a una principal.

Decir que las computadoras son imprescindibles en este tiempo es algo justo, pues, nuestra vida se ha sistematizado a tal grado que parecería que las propias computadoras han llegado a controlar la vida del hombre, pero lo cierto es que la economía, la cultura, el arte, las ciencias, la educación y en general la vida de los Estados depende de las computadoras.

A continuación hablaremos brevemente del desarrollo de las computadoras a lo largo de la historia.

1.2. LOS PRIMEROS AÑOS.

Señala acertadamente el autor Téllez Valdez:

"Desde tiempos remotos el hombre, al verse en la necesidad de cuantificar sus pertenencias, animales, objetos de caza, pieles, etcétera, ha tenido que procesar sus datos. En un principio este procedimiento fue muy rudimentario: utilizaba sus manos y almacenaba toda la información posible en su memoria".[3]

[3] ibid. p. 5.

Esta necesidad de sistematización de su información resultaba muy lenta, pues utilizaba sólo su memoria al no contar con una forma de fijación de ella en algún material.

Poco a poco fue utilizando el hombre otros recursos aparte de sus dedos, como cuentas, granos y otros objetos. Posteriormente inventó instrumentos más confiables y prácticos como el ábaco, cuya etimología proviene de la voz fenicia "abak", que significa "tabla lista cubierta de arena", el cual sigue siendo muy utilizado por algunos pueblos asiáticos como el chino, el vietnamita entre otros.

Otros instrumentos importantes que creó el hombre para sistematizar su información son: las tablas de logaritmos (de 1614); la regla de cálculo (de 1630); la máquina de pascal (de 1642); la tarjeta perforada (de 1804); la máquina de Babbage (de 1834) y el famoso Código del alemán Herman Hollerith (de 1880).[4]

La historia de las computadoras se remonta a más de sesenta años de existencia; se sabe que la primera máquina fabricada para sistematizar algún tipo de información fue la MARK I, construida entre los años de 1937 y 1944. Esta máquina se conoció también como ASCC o "Automatic Séquense Controlled

[4] Ibid. p.p. 7 y 8.

Calculator", llevada a cabo en la Universidad de Harvard con el apoyo de la poderosa empresa IBM.

La MARK I fue de hecho, la primera computadora electromecánica automática. Esta máquina realizaba largas secuencias de operaciones codificadas, registrándolas en una cinta de papel perforado y podía calcular los resultados mediante la ayuda de unidades de almacenamiento o memoria.

La MARK I tenía varios inconvenientes, entre ellos, era muy lenta, puesto que su velocidad de operación dependía de la rapidez de todos y cada uno de sus componentes (cerca de 750,000), lo cual explica su lentitud.

Esta máquina se utilizó durante quince años para llevar a cabo cálculos astronómicos.

Hablar de esta computadora en la actualidad resulta casi increíble por los contratiempos que representaba; sin embargo, debemos entender que debido a la sofisticación de estos instrumentos que se ha dado en nuestros tiempos podemos considerar que, ha sido un proceso relativamente rápido.

El segundo antecedente de las computadoras que hemos ubicado en la primera etapa, es la máquina llamada ENIAC, construida entre los años de 1943 y 1945.

La ENIAC o Electronic Numerical Integrator and Calculator, es la primera computadora electrónica desarrollada por Konrad Zuse en el Aircraft Research Institute. Esta máquina carecía de partes mecánicas, funcionando con bulbos (más o menos 18,000). Podía realizar cinco mil operaciones por segundo y su utilidad en problemas de balística y aeronáutica fue aprobada. Se dice que su único inconveniente era su tamaño, pues era demasiado grande, además, se calentaba rápidamente debido a los bulbos que utilizaba.

Posteriormente llegó la maquina llamada EDVAC (Electronical Discrete Variable Automatic Computer). Su tamaño era mayor que la anterior, era capaz de realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente.

Todas las computadoras descritas anteriormente, pertenecen a lo que el autor Téllez Valdez ha denominado como la primera generación, la cual abarca del año de 1946 (recién terminada la segunda guerra mundial) hasta 1958, construidas a base de elementos mecánicos y después mediante bulbos lo que benefició la realización de operaciones más rápidas, ahorrando energía.[5]

Dentro de esta primera etapa en el mundo de las computadoras, (1957) apareció el lenguaje de programación llamado FORTRAN (Fórmula

[5] Vid Téllez Valdez,Julio. Derecho informático. Colección: El Derecho en México una visión de conjunto. Tomo II: UNAM, México, 1991, 1112.

traductora), quizá fue el primero en su tipo y se utilizó para definir problemas mediante el uso de símbolos similares a las matemáticas.

1.3. LA ETAPA INTERMEDIA.

La segunda generación de computadoras, abarca del año de 1958 hasta 1962, se caracterizó por el desarrollo de memorias magnéticas, las cuales permitieron un registro y proceso de datos mucho más rápido,mediante una bobina de ocho pulgadas que vino a reemplazar a las más de doce mil fichas perforadas.

En esta etapa, se desarrollan otros lenguajes como el APL, el cual le permitió al hombre resolver cualquier problema matemático, aunque con un número limitado de informaciones.

Otra novedad en lo que hemos llamado la etapa intermedia, fue el uso de transistores en lugar de los bulbos de alto vacío, logrando con ello una notable reducción de espacios, pero también, se pudo obtener mayor velocidad en las operaciones y seguridad en el movimiento de los propulsores eléctricos.

Entre 1964 y 1971 surge otra generación de computadoras, (tercera generación) cuando la empresa IBM logró perfeccionar la tecnología SLT (Solid

Logic Tecnology) obteniendo de ese modo circuitos electrónicos en tamaño miniatura (un antecedente de las actuales micro chips). Asimismo, se pudieron elaborar familias de computadoras perfectamente compatibles entre sí, pudiendo realizar las mismas operaciones, las cuales alcanzaban hasta tres millones de instrucciones. Este principio sería la base de lo que hoy es Internet, una amplia red de computadoras conectadas entre sí.[6]

Poco a poco fueron apareciendo y perfeccionándose los circuitos integrados, con redes de colaboración locales, nacionales e internacionales, lo que facilitó la multiplicación de las capacidades de almacenamiento y proceso de las computadoras, la cual daría pauta para el nacimiento de Internet.

1.4. ÉPOCA CONTEMPORÁNEA.

Una cuarta generación de computadoras salen al mercado en la década de los ochentas, las cuales utilizaban componentes de muy alta capacidad, pero lo que marca una notable diferencia con sus antecesores es la utilización de chips o pastillas, es decir, micropaquetes de silicio, con una medida de casi un centímetro, con cualidades o capacidades que para esos años parecían increíbles, pero que hoy son una realidad y algo a lo que ya nos hemos acostumbrados.

[6] Ibid. p. 3.

También en esta generación se desarrollan nuevos y más completos programas de computación como el PROLOG y el LISP.

El autor Téllez Valdez dice lo siguiente:

"Hoy, las computadoras personales o P.C. (en Ingles "Personal Computers") logran ofrecer con un gasto no tan elevado, beneficios similares a los de las demás computadoras gigantescas de los 60's, permitiendo a los usuarios, la integración en circuitos con la posibilidad de conectarse con los grandes sistemas. La reducción de los costos y el aumento de la velocidad de proceso resulta notorio si se analizan los estudios comparativos que la IBM efectuó y según los cuales, un conjunto de 1,700 operaciones industriales costaba en el año de 1955, $14.54. dólares; en 1965, 47 centavos, y en 1983 solamente 7 centavos, y en cuanto a la velocidad de operaciones, se paso de 375 segundos en 1955, a 20 segundos en 1965 y a un solo segundo en 1983".[7]

Es notorio el avance experimentado en la informática en la década de los ochentas, ahorrando espacio y tamaños, además de que se pudo lograr que las máquinas tuvieran más capacidad de almacenamiento, procesamiento y respuesta a las operaciones solicitadas. Estos adelantos permitieron también lograr un considerable ahorro de dinero, lo cual hizo que las grandes compañías obtuvieron más ganancias al año.

---

[7] Idem.

También en esta generación se desarrollan nuevos y más completos programas de computación como el PROLOG y el LISP.

El autor Téllez Valdez dice lo siguiente:

"Hoy, las computadoras personales o P.C. (en Ingles "Personal Computers") logran ofrecer con un gasto no tan elevado, beneficios similares a los de las demás computadoras gigantescas de los 60's, permitiendo a los usuarios, la integración en circuitos con la posibilidad de conectarse con los grandes sistemas. La reducción de los costos y el aumento de la velocidad de proceso resulta notorio si se analizan los estudios comparativos que la IBM efectuó y según los cuales, un conjunto de 1,700 operaciones industriales costaba en el año de 1955, $14.54. dólares; en 1965, 47 centavos, y en 1983 solamente 7 centavos, y en cuanto a la velocidad de operaciones, se paso de 375 segundos en 1955, a 20 segundos en 1965 y a un solo segundo en 1983".[7]

Es notorio el avance experimentado en la informática en la década de los ochentas, ahorrando espacio y tamaños, además de que se pudo lograr que las máquinas tuvieran más capacidad de almacenamiento, procesamiento y respuesta a las operaciones solicitadas. Estos adelantos permitieron también lograr un considerable ahorro de dinero, lo cual hizo que las grandes compañías obtuvieron más ganancias al año.

---

[7] Idem.

En la década de los noventas se dan cambios importantes. Los japoneses introducen al mercado la quinta generación de computadoras, máquinas dotadas de inteligencia artificial y con una increíble capacidad de aprender y ejecutar operaciones inductivas y deductivas las cuales sólo podía llevar a cabo el hombre. De esta forma se empezó a dar una competencia impresionante entre la tecnología japonesa y la occidental, lo cual al ver las novedades niponas lanzaron al mercado inmediatamente los programas de computo "ESPRIT" y "EUREKA".

Esta competencia de mercados ha llevado a las computadoras a grandes niveles de desarrollo y de sofisticación, resultando beneficiado el hombre quien actualmente puede descansar la mayor parte de sus tareas de organización, creación y de solución de problemas a estas maquinas que han revolucionado nuestro mundo.

1.5. LOS ADELANTOS EN MATERIA DE COMPUTACIÓN.

Resulta increíble darnos cuenta del desarrollo vertiginoso de las computadoras en los últimos sesenta años, sin embargo, ese desarrollo no ha llegado a su clímax por lo que debemos esperar más novedades en este campo.

Sabemos bien que una computadora tiene que estar a la par de los adelantos de la tecnología, pues de lo contrario, fácilmente cae en la obsolescencia y con ello, su capacidad de respuesta resulta más lenta. Es así, que las grandes compañías han lanzado máquinas llamadas escalables, es decir, que se pueden ir actualizando año tras año, equipándolas con programas y aditamentos de moda para estar siempre a la vanguardia.

A continuación hablaremos de estos adelantos en materia de computadoras.

1.5.1. LA SOFISTICACIÓN DE LAS COMPUTADORAS.

Basta acudir a una tienda de artículos de computación para darnos cuenta del gran avance en este campo. Actualmente las empresas fabrican para todos los bolsillos, inclusive hay comercios donde se arman las computadoras a la vista del cliente. Igualmente, se venden máquinas llamadas escalables, esto es, como mencionamos anteriormente, aquellas que pueden ser superadas año tras año para no caer en la obsolescencia. También los programas o software se han multiplicado y modernizado, puesto que las computadoras son hoy en día una necesidad para la mayoría de la gente, aunque su costo todavía no es muy accesible para la población de escasos recursos.

Las P.C. actuales (o personal computers) salen al mercado cada vez más equipadas tanto en hardware como en programas o software. En este rubro, la existencia de las computadoras "lap top" cuyo tamaño es más reducido de las P.C., ha revolucionado este campo, pues con la medida y peso de un portafolio resulta muy práctica para ser llevada a cualquier parte, por lo que es muy común ver personas que viajan con sus lap top, aprovechando el tiempo de la travesía para continuar trabajando en sus proyectos o deberes.

Sin embargo, como ya dijimos, las computadoras que hoy nos asombran y parecen extremadamente sofisticadas, el día de mañana serán superadas, sin lugar a dudas.

1.5.2. EL INTERNET.

Dice Oliver Hance:

"A fines de la década de los sesenta, el departamento de la Defensa de los Estados Unidos creó la ARPA (Advanced Research Project Agency) con la finalidad de llevar a cabo el objetivo estratégico, todavía sencillo, de asegurar el envío de la orden de abrir fuego desde el centro de control a las bases de misiles y de hecho, especialmente si las redes de comunicaciones hubiesen

quedado en parte destruidas por un ataque. Esta misión se extendió con rapidez para incluir acceso y para poder compartir todos los recursos de cómputo de Estados Unidos. La nueva red se denominó ARPANET "[8]

El mismo autor dice que Internet es:

". . . . . una federación de redes que está en constante desarrollo y que, en la actualidad, es de acceso general".

Víctor Manuel Rojas Amandi señala lo siguiente sobre Internet:

"Internet es un sistema maestro de diversas redes de computación que cumple dos funciones básicas: medio de comunicación y medio de información.

Como sistema de redes de cómputo, Internet presenta una característica especial: cualquier computadora puede conectarse al sistema. Para ello, solo se necesita contar con un programa de computación TCP/IP . . . . ."[9]

Después agrega el autor:

" Como medio de comunicación, Internet ofrece una amplia gama de canales de enlace, entre los que se hallan la comunicación escrita (por ejemplo, el

[8] Hance. Oliver. Leyes y Negocios en Internet. Editorial Mc Graw hill. México. 1997. p. 40.

[9] Rojas Amandi. Víctor Manuel. El uso de Internet en el Derecho. Editorial Oxford. México. 1991. p.1.

e-mail), la comunicación verbal (contrato por teléfono y chat de voz) e incluso comunicación visual (téleconferencia en Internet).

Como medio de información; Internet puede compararse con una gran biblioteca, a cuya sala de lectura es posible acceder desde cualquier computadora conectada al sistema. Sin embargo, a diferencia de la biblioteca donde sólo las autoridades están facultadas para introducir libros o documentos, el sistema Internet permite que los usuarios agreguen información al acervo, lo que contribuye al mayor crecimiento de la información"

Internet es una compleja estructura o red de redes que interconecta a muchas computadoras entre sí, facilitando el intercambio de información entre ellas.

Una red se forma cuando dos o más computadoras se conectan entre sí, permitiendo el intercambio de la información. Al enlazarse varias computadoras a manera de red, todas podrán acceder y usar simultáneamente los archivos y programas que tienen cada una por separado, pero, en una de las computadoras de la red se concentran los principales archivos, convirtiéndose en una computadora central que recibe el nombre de servidor, y las otras conectadas entre sí se les llama clientes. Paulatinamente, el servidor, de una red se puede conectar al de las otras redes creándose una gigantesca red de redes.

Internet ha revolucionado aún más nuestro mundo. Es un programa "sui generis" o especial que le permite al usuario navegar a través de la red y conectarse con cualquier país por alejado que se encuentre en cuestión de segundos.

Internet es una compleja red que puede acceder a cualquier tópico o tema, pero carece de regulación legal tanto nacional como internacional.

En sus orígenes, Internet no fue concebido como una red de cómputo, sino por la satisfacción de ciertas necesidades del Departamento de Defensa de los Estados Unidos.

Dice el autor Rojas Amandi:

"Para lograrlo, se necesita una red que no fuera dependiente de una sola computadora central. Esto es importante, pues el concepto original de red de computadoras exige una computadora central (servidor) que administre la información y esté al servicio de los usuarios enlazados con la red. Éste es el sistema de red de computadoras que los juristas veían de manera habitual en los centros de trabajo antes de Internet"[10]

[10] Ibid. P. 2.

Para los Estados Unidos, un sistema tradicional con una red dirigida por una computadora central resultaba muy vulnerable a los expertos del citado Departamento de la Defensa de ese país, pues un ataque a la computadora central significaría la caída de toda la red; es así que, a partir de los sesentas se desarrolló una red que no dependiera de un sólo servidor y que se organizará de tal manera que cada computadora funcionara de forma independiente en relación con otras. Así, al obtener la información en cualquiera de las computadoras enlazadas al sistema, se evitaría el riesgo de que el daño que pudiera sufrir una computadora especifica dañara todo el sistema.

Nace ese sistema que originalmente se llamo APARNET, el cual funcionó con un programa de computación llamado NPC (Network Control Protocol) que hizo posible el uso descentralizado de la red. En la década de los sesenta APARNET creció más de lo esperado, debido a que varias redes científicas se enlazaron al sistema. Científicos y profesores de los Estados Unidos comenzaron a considerar la posibilidad de trasmitir mensajes electrónicos mediante la red, participando en el desarrollo de proyectos científicos.

En década de los ochentas, el NPC fue sustituido por un programa nuevo llamado TCP/IP, que trabaja más eficazmente, pues convierte los datos enviados mediante Internet en pequeños paquetes que manda a su lugar de

destino con base en sus direcciones, a través de diferentes puntos de enlace de Internet y de la computadora destino que los recompone.[11]

En esa misma década Internet se separa de APARNET y se desliga también de objetivos militares, perfilándose como un medio de comunicación e información científica y educativo.

A pesar de que la National Science Fundation Network trató de impedir que Internet fuera usado como red de comercio, no tuvo mucho éxito, pues la posibilidades de la red en esta materia no eran muchas. De manera que desde el año de 1995, el gobierno de los Estados Unidos decidió privatizar y no otorgar más subsidios a la red y desde ese año, es posible utilizar este sistema para objetivos de diversa índole, llegando a hacer lo que hoy es: una inmensa red de redes multitemática.

Internet es una gran posibilidad de desarrollo, tanto para los Estados como para las personas, siendo para estas últimas, incluso, un estilo de vida, pues a través de la red se pueden hacer operaciones bancarias, bursátiles, contratos de compraventa de todo lo imaginable lícito o no, sin necesidad de salir de casa. Internet ha traído ante nuestros ojos una cultura nueva, la comunicación virtual, con las funciones de " e-mail " y de "chat ", la gente se conoce, relaciona y comunica a través de las computadoras.

---

[11] Idem.

1.5.3. LOS VARIADOS PROGRAMAS COMPUTACIONALES.

Para comprender mejor el tema que abordamos debemos señalar que el autor Julio Téllez Valdez menciona:

"Para que las computadoras puedan funcionar en los términos adecuados es necesaria la utilización de los llamados lenguajes de programación, como aquellos medios que permiten la comunicación entre el hombre y la máquina, es decir, entre la computadora y el usuario"[12]

Otra opinión más, P. Guirao dice:

"Programa. Conjunto de instrucciones escritas en un lenguaje de ordenador y encaminadas a que éste realice una tarea especifica".

"Programación. Conjunto de instrucciones escritas en lenguaje de programación que ordena el procesador que realice diversas operaciones con los datos contenidos en el programa o suministrados por el usuario. Los programas

[12] Téllez Valdez, Julio. Op. Cit. P. 12

van desde los que llevan la contabilidad de las empresas, hasta los que convierten el ordenador en un juego de video"[13]

Actualmente las computadoras necesitan imprescindiblemente contar con varios programas adaptados para poder realizar las tareas encargadas por el hombre, esos programas reciben el nombre de software y existen muchos en los establecimientos de venta de artículos de computación.

Hay programas útiles para el campo jurídico como Word, Windows en sus variadas versiones (95, 98, ME, XP). Otros programas que se utilizan en áreas como contabilidad son Excell, Basic, Power Point, etc.

Sin los programas antes descritos sería muy complicado que las computadoras pudieran realizar desde labores simples, hasta las más sofisticadas como gráficas, tablas de estadísticas o presentaciones de trabajo en movimiento.

1.6. NUESTRA SOCIEDAD Y LAS COMPUTADORAS.

En puntos anteriores dijimos ya, que nuestra sociedad se encuentra supeditada a la cibernética, la cual parece regir nuestra vida. Se quiera o no, lo real es que nuestro diario acontecer depende del uso de las computadoras: en la

[13] ibid.

casa al organizar nuestras actividades; en la escuela, en la oficina, en el Banco o al hacer una simple compra en un supermercado, etcétera; aún más, las economías de los países dependen del uso de las computadoras, esto sin contar las variadas operaciones bursátiles y bancarias que a diario se realizan por Internet.

A continuación abundaremos en la trascendencia de las computadoras en nuestra sociedad.

1.6.1. LOS BENEFICIOS DE LAS COMPUTADORAS EN LA VIDA DIARIA, EN EL TRABAJO, LA CIENCIA, LAS ARTES Y LA DIVERSION.

Posiblemente hace diez años o más, nos era raro encontrar computadoras en los diversos lugares que frecuenta la gente, posiblemente se pensaba que su utilización era un lujo. En los tiempos actuales esto ha cambiado, puesto que en diversos comercios o negocios, ya sean pequeños, medianos o grandes, en las escuelas públicas o privadas, en los Bancos, en las oficinas de Gobierno tanto Locales como Federales, en las clínicas de salud del sector público y privado, así como los lugares destinados a la diversión se utilizan computadoras y diferentes programas que permiten a los usuarios llevar a cabo un control seguro

y adecuado de sus actividades, brindando así un mejor servicio al público consumidor.

Aún cuando debemos tener presente que no todas las familias mexicanas cuentan con una computadora en su casa, porque su precio no está todavía al alcance de las familias más necesitadas o atrasadas; muchas de ellas han hecho un esfuerzo económico para contar con una computadora en casa para diferentes fines, tales como, tareas escolares; trabajos universitarios o de oficina; llevar la administración de la casa, etc.

Es indudable que las computadoras han hecho gran parte de nuestra vida más fácil, al simplificar trabajos, operaciones o simplemente al sistematizar información que de otra manera resultaría muy complicado clasificarla y tenerla disponible en cualquier momento. El uso de estas máquinas le ha ahorrado tiempo, gastos y problemas al ser humano, con lo cual, el costo de las mismas pasa a justificarse plenamente.

Por otra parte, sin las computadoras sería complicado el difundir las ciencias, las artes e inclusive, la diversión, puesto que como también lo dijimos, Internet es el medio de expresión, de comunicación masiva y de información más rápido del mundo, pues en sólo segundos el interesado puede explorar museos, tiendas, o compañías en Europa, Asia, etcétera; sin tener que desplazarse hasta esos lugares.

1.6.2. LA SISTEMATIZACIÓN DE NUESTRA VIDA. CONVENIENCIAS E INCONVENIENCIAS.

La sistematización de nuestras vidas nos ha dado la facilidad de cumplir con nuestras tareas o deberes ahorrando tiempo, esfuerzo y con pocos recursos: una o varias computadoras; sin embargo, tanto adelanto trae consigo algunas inconveniencias tales como que el ser humano ha dejado de hacer esfuerzos para realizar sus tareas diarias como por ejemplo, buscar un libro y leerlo, puesto que hoy, Internet va a localizar el libro deseado para que pueda obtenerse una copia del mismo. Otro inconveniente en el rubro de la educación es que muchos alumnos de todos los niveles ya no se ven en la necesidad de acudir a las bibliotecas de sus escuelas o las públicas, ya que al acudir a Internet pueden obtener la información que necesitan y así cumplir con sus trabajos escolares.

El uso de Internet ha dado la posibilidad de entablar nuevas amistades o inclusive de aspirar a encontrar una pareja sin importar la edad, el país, la preparación académica o condición económica mediante el uso del llamado "chat", lo cual simplifica distancias pero condiciona y engaña en ocasiones a los interesados quienes sólo cuentan con información que la otra parte quiera proporcionar, siendo muy común que los datos sean falsos y con ello se creen problemas personales.

En este orden de ideas, la sistematización de nuestra sociedad ha traído una marcada dependencia de las computadoras, sin las cuales, resulta difícil entender nuestra vida diaria. Dentro de esta relación inseparable hombre-computadora partiremos para hablar de los virus informáticos, un tema de gran novedad e importancia y que ha causado muchos daños económicos. Inclusive, ha sido considerado por muchos como una forma o clase de terrorismo "virtual".

CAPÍTULO 2

ASPECTOS GENERALES DE LOS VIRUS INFORMÁTICOS.

2.1. CONCEPTO DE INFORMÁTICA.

Señala José Antonio Padilla Segura que:

"Es casi por todos sabido que el termino informática tiene su origen en Francia. Quienes lo gestaron como neologismo uniendo a las dos primeras silabas del término information, las tres últimas de automatique con lo que este vocablo de nuevo cuño, en su momento, daba a entender claramente la intención de referirse a un proceso de información automatizada. En forma más explícita quiso significar el tratamiento automático de los datos que constituyen la información"[14]

Estas palabras son corroboradas por el autor Julio Téllez Valdez al decir lo siguiente:

[14] Padilla Segura, José Antonio. Informática Jurídica. Editorial Instituto Politécnico Nacional. México, 1991. p.5.

"La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962"[15]

De esta forma, la voz informática se compone de la unión de los vocablos información y automatización hasta convertirse en el termino que hoy es usado en materia de computadoras.

A continuación pasaremos a dar un concepto de esta disciplina:

Téllez Valdez dice:

"En el sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una toma de decisiones"[16]

El propio Téllez Valdez cita en su obra dos opiniones más:

Mora y Molino dicen que es:

". . . . . el estudio que delimita las relaciones entre los medios (equipo), los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado"

[15] Téllez Valdez, Julio. Op. Cit. P.5.
[16] Idem.

Mario G. Lozano dice que la informática se caracteriza:

". . . . como producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un pleno disciplinario."

José Antonio Padilla Segura, sabedor de la dificultad de dar una definición o concepto de informática manifiesta:

"Desde mediados de los años sesenta se vienen sucediendo los intentos más o menos felices de encontrar una definición o hacer una buena descripción de lo que es la informática. La realidad es que a medida que el tiempo ha trascurrido, esto que fue una disciplina o una rama de la ciencia y de la técnica, se ha convertido en un complejo campo de conocimientos, de experiencias y de aplicaciones, en todas las tareas del quehacer humano. Es por ello que no es fácil aplicarle una definición integral"[17]

El mismo autor nos ofrece su propia definición:

"Conjunto de disciplinas técnicas para la elección, captación, almacenamiento, procesamiento, organización y reparación de datos a fin de contar con una información eficiente y con una comunicación eficaz dentro de un

[17] Padilla Segura, José Antonio. Op. Cit. P.5

sistema, sea político, social o económico, tratados en forma racional, generalmente empleando medios o recursos automatizados o de difusión; tales como son las computadoras y los sistemas modernos de telecomunicación, para aplicarlos a la compresión de situaciones y a la solución de problemas".

Puntualizando lo anterior concluiremos diciendo que la informática es una disciplina compuesta por un conglomerado o conjunto de técnicas utilizadas para sistematizar de forma lógica y automática cualquier tipo de información la cual habrá de ser utilizada por el interesado en la toma de decisiones.

2.2. CONCEPTO DE VIRUS INFORMÁTICO.

Hemos señalado que en las últimas tres décadas, la informática y todos sus contenidos han experimentado un notable avance, inclusive, podemos calificarlo como vertiginoso, creándose computadoras más potentes, de respuesta mucho más rápida y que satisfacen las necesidades de trabajo de empresas, instituciones oficiales y de las personas en general. De la misma forma, se han creado programas computacionales o "software" que enriquecen las capacidades de las computadoras y hacen más fácil la vida diaria del hombre. Sin embargo, dicho avance ha traído también la creación de mecanismos o programas tendientes a causar daño a los usuarios de la red de Internet, lo que constituye

uno de los principales inconvenientes y peligros de la súper carretera de la información llamada Internet. A este tipo de programas destinados a dañar los archivos que obran en la computadora de otras personas se les conoce como **"virus informáticos"**.

Los virus informáticos se han multiplicado rápidamente, al igual que otros programas cuya utilidad es manifiesta. Muchos de ellos han cobrado fama debido a que su propagación es realmente fácil y rápida, por lo que en cuestiones de minutos llegan a las computadoras de otros países.

A continuación procederemos a explicar qué es un virus informático, y cómo se crean.

Un virus informático es un programa o código, en ocasiones complejo y la mayoría de las veces es realmente muy simple. Su único objetivo es entrar en el sistema del ordenador (Computadora), duplicarse y propagarse a todos los archivos que sea posible, sin que el usuario tenga conocimiento de ello, hasta que es muy tarde y el virus haya conseguido su meta: dañar los archivos informáticos que obran en el equipo, lo cual puede causar un severo daño en el mismo.

Tenemos otra opinión de virus informático:

"Un virus es un programa creado con el fin de realizar una función

en particular, generalmente perjudicial para una computadora, un sistema o una red. El perjuicio puede ser en contra de la información o la seguridad de las máquinas infectadas. Una de las características más importantes de un virus es que se puede auto-duplicar las veces que quiera; de la misma forma puede programarse para pasar inadvertido, incluso disfrazarse de un archivo inofensivo hasta que llega el momento de ejecutarse y armar el relajo.....".[18]

Este concepto nos parece más completo, pues ofrece otra clase de información que debe ser analizada a efecto de poder comprender en toda su magnitud los alcances de los virus informáticos. Así, encontramos en la revista citada que un virus es un programa de cómputo creado con el fin de causar daño a una o varias computadoras, a los sistemas o las redes de ellas. El perjuicio que puede causar el virus puede ir contra los archivos de información que están dentro de una o varias computadoras o contra la seguridad de los equipos infectados. Un virus es capaz de auto duplicarse muchas veces; puede también alojarse durante algún tiempo en una o varias computadoras y permanecer en estado de latencia hasta que el usuario abra el archivo, momento en el que le permitirá salir al virus e infectar los demás archivos, dañarlos e inclusive, afectar la seguridad de la máquina misma u ordenador (como se le nombra en España). El virus informático puede adoptar la forma de un archivo totalmente inofensivo y así confundir al usuario quien fácilmente le permitirá salir y cumplir su cometido.

---

[18] Revista "www Vivir en Internet". Publicación mensual, 09/2001. México. 2001. p. 59.

Tal ha sido el caso de ciertos virus informáticos que han cobrado fama mundial, como por ejemplo: " I love you " o el "virus Kurnikova", también conocido como "virus VBS" o " virus SST", el cual prometía a los usuarios encontrar una fotografía de la famosa tenista rusa desnuda, congestionando en pocas horas los servidores de correo electrónico en Europa y América del Norte. Otro caso interesante fue el del virus llamado "Fw: Naked Wife", un virus que se hace pasar por un archivo creado con el programa Flash de Macromedia. El cuerpo del mensaje dice en idioma inglés: "Mi esposa nunca luce así¡ Saludos", después agrega el nombre de pila del remitente y una vez libre el virus intenta borrar cualquier archivo. Otro virus extremadamente peligroso es el llamado "Homepage", el cual a diferencia de los demás no recurre a la intriga sexual sino que una vez liberado, trata de abrir numerosos sitios de Internet calificados como pornográficos. Este virus tiene una finalidad destructiva mínima, pero tiene la capacidad de colapsar los servidores de correo electrónico.[19]

Se desprende de todo lo anterior que los creadores de virus informáticos son personas con amplios conocimientos de computación, de programas y sobre su propagación y alcances, los cuales se valen de astucias o engaños de tipo sexual, principalmente, para que los usuarios caigan en la trampa y dejen salir los virus alojados en sus equipos y causar daños que pueden ser leves o muy serios.

[19] Vid. www.cnnenespañol.com.

El término virus informático tiene un sentido metafórico o virtual, como si realmente se tratase de un conjunto de microorganismos unicelulares o pluricelulares que se alojan en el cuerpo humano y que causan alguna enfermedad. Se ha considerado que gracias al enorme parecido con los programas informáticos creados para causar daño en los archivos y en la seguridad de los equipos de cómputo, a su desarrollo, etc, son virus, hablando virtualmente.

2.3. ALGUNOS ANTECEDENTES DE LOS VIRUS INFORMÁTICOS EN EL MUNDO.

Realmente, el origen de los virus informáticos es muy reciente al igual que las computadoras mismas. Según algunos datos su nacimiento se remonta a finales de los años sesentas, cuando los norteamericanos Douglas McIlory, Victor Vysottsky y Robert Morris idearon un juego llamado: "Core War" , el cual se convirtió rápidamente en el pasatiempo de algunos de los programadores de los laboratorios Bell de la industria AT&T . Como se desprende de su nombre, "Core War" era una batalla en el core o memoria de la computadora, en el que dos jugadores escribían cada uno un programa llamado organismo, cuyo hábitat era precisamente la memoria del ordenador. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida. El primero que lo

consiguiera ganaría el juego. Una vez terminado el juego, se borraría todo rastro de la batalla de la memoria de la máquina. Se cuenta que este tipo de entretenimientos se sancionaban por los superiores de esa compañía por considerar que era muy peligroso que se dejara un organismo suelto (programa computacional), que pudiera acabar con las informaciones que habrían de aplicarse el día siguiente. Esto ocasionó que el juego se efectuara de forma clandestina.

"Core War" es casi desconocido para la mayoría de las personas que estaban relacionadas con la informática, lo cual significa que no tuvo mucha difusión como un juego. Se cuenta que en 1987 un periodista de los Estados Unidos perdió la información de seis meses de trabajo que tenía guardada en un disco, al tratar de recuperarla pudo darse cuenta de que se trataba de un acto de sabotaje. Casualmente, en el disco se encontraba un número telefónico de una tienda de computación de Pakistán y el mensaje siguiente:

"Bienvenidos al calabozo.....llámenos para la vacuna!".

La información del periodista había sido víctima de un virus maligno.

Se hicieron algunas investigaciones y se pudo concluir que la tienda a la que se hacía referencia era "Brain Computer Services", la cual se dedicaba

entre otras cosas a vender copias ilegales de algunos programas muy caros con un precio de $1.50 cada uno, lo cual ya nos muestra que desde entonces se realizaban actos de piratería que no son originarios de nuestro país, los cuales tuvieron éxito debido al considerable ahorro que representaba para el consumidor el comprarlos ilegalmente. Durante los años de 1986 y 1987, algunos de los clientes de esta tienda fueron precisamente algunos estudiantes de los Estados Unidos, quienes eran atraídos por el bajo costo de los programas. No obstante, escondido en el disco se encontraba un virus, por lo que cada vez que el programa era abierto y ejecutado, el virus contaminaba a la computadora y ésta a su vez, infectaba a los discos de otros usuarios. Cabe destacar que los diseñadores de los virus fueron los hermanos Amjad y Basit Farooq Alvi, quienes eran los dueños de la tienda de computación referida de nacionalidad pakistaní. En 1985 los hermanos Amjad Alvi, decidieron hacer un software, sin embargo, sorpresivamente el software fue copiado y usado sin su permiso. De esta forma se cuenta que Amjad ideó un programa que pudiera autoduplicarse y cuya función fuera la de infectar la computadora de un usuario que no contara con autorización de los creadores del programa, con lo que el mismo se vería en la necesidad de llamarles para reparar los daños.

Tiempo después, los hermanos Farooq Alvi tenían un virus que incluían en sus copias ilegales, y sucedía que cuando un pakistaní deseaba una

copia del programa se le vendía libre de virus, pero cuando se trataba de un extranjero, se le vendía una copia contaminada.

Según declaraciones de los hermanos Alvi, en su país las leyes del Derecho de Autor no incluyen el software, por lo que vender copias piratas no constituye un delito, contrariamente con la mayoría de las legislaciones del mundo, como la de los Estados Unidos y la de México, donde se prohíbe este tipo de prácticas, al menos teórica y jurídicamente, puesto que en la realidad constituye un modo de vida de muchas personas el realizar copias piratas de casi todos los programas de moda o que representan alguna utilidad para los usuarios y cuyo costo normal es muy alto.

Sobre nuestra Ley Federal del Derecho de Autor y la protección de los programas de cómputo, tenemos lo siguiente:

"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".

Finalmente, el artículo 106 habla de los derechos que la Ley le concede al autor del programa de cómputo:

"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 descompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje".

Los programas de computación deberán ser inscritos en el Registro Federal del Derecho de Autor para que surtan efectos contra terceros "erga omnes".

Finalmente se cuenta que los hermanos Alvi dejaron de vender copias ilegales en el año de 1987, advirtiendo que había sido una lección para los piratas.[20]

Resulta entonces entendible imaginar que aquél juego de entretenimiento se habría de convertir en una poderosa arma capaz de colapsar y dañar los archivos de millones de usuarios en todo el mundo, ya que a través de Internet es posible que lleguen hasta los confines del planeta en sólo cuestión de minutos o segundos, cundiendo el pánico entre los mismos usuarios y causando un detrimento patrimonial que puede llegar a estimarse en millones de dólares.

En la actualidad existen muchos virus informáticos, pues su propagación es relativamente fácil. Posiblemente estamos ante una nueva forma de terrorismo mundial que en cualquier momento pone en jaque a las instituciones económicas, financieras y políticas del orbe.

[20] Vid. López-Ortíz, Alex y Daniel M. Germán, en América on line México. www.americanoline.com.mx. Lunes 02 de julio de 2001.

2.4. CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS.

A la fecha existen ya algunos estudios sobre virus informáticos. Gracias a ellos es que podemos advertir la existencia de diferentes tipos o clases de ellos.

Hemos dicho que un virus informático es un programa diseñado para replicarse y distribuirse por si mismo, sin que el usuario del equipo contaminado se de cuenta. Estos virus se distribuyen adhiriéndose a otros programas (como sus programas de procesamiento de palabras u hoja de cálculos: word, excell o outlook, entre otros) o en el sector de arranque de un diskette. Cuando un archivo que ha sido previamente infectado es ejecutado, o la computadora es arrancada desde el diskette infectado, el virus es automáticamente también ejecutado. Es normal que el virus se esconda en la memoria del ordenador, esperando infectar al próximo programa que corra, o el próximo disco accesado.

Muchos virus pueden mostrar un mensaje en cierta fecha, borrar archivos después de que el programa infectado ha corrido un cierto número de veces. En estos casos, estamos ante efectos benignos, pero hay otros en los que los efectos son detrimentales y molestos, reduciendo la velocidad del sistema,

causando cambios menores en la pantalla de la computadora. Algunos virus más, son realmente amenazadores, al causar la caída del sistema, archivos dañados e inclusive, la pérdida de información.

Citemos otro caso o ejemplo de virus, el famoso "SirCam", mejor conocido como: "hola como estas", del cual encontramos que:

"Recientemente el mundo fue infectado por un famoso virus: 'SirCam'. Por si acaso no tienen computadora (o se fueron de vacaciones y no se enteraron), les diré que este virus es tan práctico y de tan veloz propagación, que antes de ser noticia mundial ya se había encargado de dar de baja (temporalmente) servidores de mails de compañías transnacionales para ser desinfectados.

Si observamos de cerca al SirCam, podemos encontrar algo interesante: este virus es bilingüe. Afortunadamente no es bilingüe e inteligente, sólo bilingüe, y se basa en la terminación de la dirección de correo para enviar mensajes en inglés en los casos de dominio.com, o en español en los casos de dominio.com.mx. El mensaje dice lo mismo, en ambos idiomas, y al parecer, el original podría ser el escrito en español. Súmenle a esto el curioso dato de que este virus fue programado para usar un servidor de mail ".com.mx" en caso de que

la víctima no tuviera uno válido, y podemos crear el rumor de que el "SirCam" es un virus mexicano....[21]

Algunos datos estadísticos son asombrosos, por ejemplo, en 1986 sólo se conocía la existencia de un virus informático en todo el mundo. En la actualidad, se estima que existen casi 4,8000 virus en todo el mundo, con nuevos ejemplos y variantes, entre 70 y 100 de ellas que aparecen cada semana. Un dato alentador es que de los 4,8000 virus muy pocos están en libertad.

Estos son algunos de los tipos o clases de virus informáticos en la actualidad:

Infectores de Archivos:

Son virus que se pegan de (o reemplazan) archivos .COM y .EXE, aunque en algunos casos infectan archivos con extensiones. SYS, .DRV, .DLL, .BIN, .OVL y .OVY. Con estos virus, los programas sanos usualmente se infectan cuando son ejecutados con el virus en la memoria. En otros casos, son infectados al ser abiertos o el virus simplemente infecta a todos los archivos desde el que fue corrido.

Dentro de esta categoría de virus están también los infectores del Sector de Arranque: cada drive lógico, tanto discos duros como floppies, contiene

---

[21] Revista "www Vivir en Internet", Op. Cit. P. 61.

un Sector de Arranque, el cual contiene información específica acerca del formato del disco y los datos almacenados en él, y contiene un pequeño programa llamado precisamente "Programa de Arranque" (que carga los archivos de sistema del MSDOS). El Programa de Arranque muestra el mensaje "Non-system Disk or Disk Error", si los archivos de sistema del MS-DOS no están presentes.

Una computadora se puede infectar con un virus del Sector de Arranque, dejando un diskette infectado en el drive de arranque y encendiéndola. Cuando el Programa de Arranque es leído y ejecutado, el virus entra en la memoria e infecta al disco duro de la computadora. Hay que tener presente que cada disco contiene un Sector de Arranque, por lo que es posible y común infectar una máquina con un disco de datos.

Infectores del Récord Maestro de Arranque:

El primer sector físico de cada disco duro (Lado 0, Track 0, Sector 1) contiene el Record Maestro de Arranque (Master Boot Récord) y la Tabla de Partición. El citado Récord Maestro de Arranque (MBR) contiene un pequeño programa llamado "Programa Maestro de Arranque", el cual busca en la Tabla de Partición, los valores para la localidad inicial de la Partición de Arranque, y ordenándole al sistema ir allí y ejecutar cualquier código que encuentre a su paso. En los floppies, los mismos virus mismos infectan los Sectores de Arranque.

Una computadora se puede infectar con un virus del Récord Maestro de Arranque en la misma forma en que se infecta con un virus del Sector de Arranque, es decir, dejando un diskette infectado en el drive de arranque y encendiendo la computadora. Así, cuando el Programa del Sector de Arranque es leído y ejecutado, el virus entra en memoria e infecta el MBR de su disco duro.

Infector Directo:

Un virus estará activo sólo cuando un archivo infectado está siendo ejecutado.

Infector Residente en Memoria:

Un virus Infector Residente en Memoria es similar a un programa convencional que termina y permanece residente en memoria (TSR), toma control del sistema y continúa infectando mientras se use la computadora, incluso si se cierra el programa infectado. El virus mantiene el control hasta que la memoria de la computadora sea limpiada, re-iniciándola "en frío" o con un "Reset".

Virus Polimórfico:

Es un virus que deliberadamente cambia su propio código de programación para impedir que sea detectado. Cada archivo infectado por un virus de este tipo contendrá un conjunto diferente de instrucciones, aún en el caso de que todos ellos estén infectados por el mismo virus.

Virus Escondido (Stealth):

Es un virus programado para que activamente busque encubrirse contra su detección, o bien, que es capaz de defenderse contra los intentos de analizarlo o removerlo. Estos virus contienen una ingeniería especial que les permite eludir la detección con herramientas antivirus tradicionales. Esto lo logra quedándose en la memoria después de ejecutarse. Desde allí monitorea e intercepta las llamadas del sistema operativo. Cuando el sistema intenta abrir un archivo infectado, el virus escondido le muestra la versión no infectada, escondiéndose de esta manera.

Inclusive, algunos detectores de virus, usando las técnicas tradicionales, pueden de hecho propagar el virus. Esto es porque abren y cierran los archivos para revisarlos, lo que da al virus oportunidades adicionales para propagarse. Los detectores también fallan al encontrar al virus, porque en el momento de abrir el archivo para la detección, se causa que el antivirus temporalmente desinfecte el archivo, haciéndolo aparecer como normal.

Gusano:

Los "gusanos" de computadoras son programas que pasan de computadora a computadora por medio de una red (como por ejemplo, Internet). A diferencia de los virus explicados anteriormente, no infectan programas, diskettes o archivos con capacidad para macros. En su lugar, hacen copias de si mismos y

las envían a través de la red hacia otras máquinas. Los "gusanos", provienen al igual que los virus de fuentes anónimas o no localizables.

Están frecuentemente equipados con descifradores de passwords basados en diccionarios y otras herramientas tipo "cracker" que les permiten penetrar en otros sistemas. Se dice que los gusanos con frecuencia roban o vandalizan los datos en una computadora.[22]

2.5. LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS. PROCEDIMIENTO.

Anteriormente hemos hablado ya sobre la forma en que se crean y se propagan los virus informáticos, por lo que sólo redundaremos sobre el tema.

Es un hecho que los virus son en la actualidad una pesadilla que amenaza a la mayoría de los usuarios de equipos informáticos, y no sólo a aquellos que tienen acceso a redes como Internet, ya que como dijimos, una máquina se puede infectar al introducirle un diskette previamente infectado. Realmente constituye un serio problema que pone en jaque a todos los usuarios de las computadoras en el mundo.

[22] López-Ortíz, Alex y Daniel M. Germán en América on line México. www.aol.com.mx. Lunes 02 de julio de 2001.

Hemos dicho también que un virus es un mini programa de computación que funciona dentro de la computadora, son diseñados para causar daño en los archivos existentes e incluso pueden dañar seriamente a la computadora. Hay otros virus que su finalidad no es precisamente la de causar daño pero son los menos, por ejemplo, los diseñados para hacer bromas molestas, como el desplegar un mensaje insolente; el hacer correr un ratón rojo a través de la pantalla o el desplomar las letras del texto que se está escribiendo, como si fuera una cascada. Como vemos, aún en estos casos, se ocasiona un daño en cuanto a la pérdida de tiempo y posiblemente de información, si ésta no está asegurada o guardada debidamente.

Los virus son creaciones de personas programadoras deseosas de causar daño, el cual puede ser leve o serio.

Dijimos igualmente que los virus adoptan ese nombre porque actúan de la misma manera que un virus biológico; se introducen en la computadora, se reproducen allí y acaban destruyendo los datos de la misma en la que se han alojado, como sucede con los virus biológicos. Se transmiten de una computadora a otra, mediante archivos compartidos o transferidos desde Internet que es la forma más rápida y común de hacerlos llegar a otros equipos en el mundo en sólo cuestión de minutos. Podríamos decir que si una computadora permaneciera

aislada de otras, posiblemente no adquiriría algún virus, aunque ello no es totalmente seguro, pues si se introduce un diskette contaminado en ella, inmediatamente se contaminará.

Por otra parte, muchos personas suelen tener en su computadora algún virus sin saberlo, por lo que al enviar a sus conocidos archivos infectados, les causarán daños quizá irremediables.

La mayoría de los virus biológicos nacen en algún laboratorio. En términos generales, el código de los virus es escrito y publicado por los llamados "hackers" que se jactan de su trabajo, o por investigadores y creadores de antivirus.

Los virus encuentran la mejor manera de esparcirse y llegar a otras computadoras en la red de redes llamada Internet, ya que en la red se auto esparcen y auto envían a todas las direcciones de "e-mail" que aparecen en la libreta de direcciones de la computadora en la que se encuentran.

Acerca de la forma en que actúan los virus tenemos lo siguiente:

El virus entra a la computadora como parte de un archivo de programa infectado (COM, EXE o del sector de arranque). Anteriormente, los virus

viajaban casi exclusivamente a través de la distribución de diskettes infectados. En la actualidad, los virus se descargan con frecuencia de redes (incluyendo Internet), por ejemplo, como parte de los archivos de configuración de un programa de prueba, como una macro para un determinado programa o como un archivo adjunto a un mensaje de correo electrónico. El "e-mail" o coreo electrónico no es en sí un virus, sino el medio de trasmisión, pues éste es un programa que debe ser ejecutado para estar activo.

Un virus inicia su vida y su labor destructiva como un programa similar al caballo de Troya, es decir, se oculta dentro de otro programa o archivo y se lanza con él. En un archivo ejecutable infectado, el virus ha modificado esencialmente el programa original para apuntar al código del virus y así lanzar ese código junto con el propio. De esta forma, salta el código del virus, lo ejecuta y después de ello salta de nuevo al código original. En este momento el virus está activo y el sistema infectado.

Una vez activado, el virus hace su trabajo inmediatamente (si se trata de un virus de acción directa), o se coloca en segundo plano como programa residente en memoria, utilizando el procedimiento TSR (Terminate and Stay Resident: termina y permanece residente) permitido por el sistema operativo. La mayoría de los virus son de este tipo, es decir, residentes, dada la amplia gama de actividades permitidas por los programas TSR.

Los virus del sector de inicio o los que infectan los archivos residen en determinadas zonas del disco duro de la computadora, siendo leídos y ejecutados por el ordenador en el momento del arranque. Las dos zonas del disco duro se leen durante el proceso de arranque, en el cual el virus se carga en memoria. Los virus pueden infectar los sectores de arranque de los discos flexibles, pero normalmente un disco de arranque libre de virus y protegido contra la escritura, ha sido casi siempre una forma segura de iniciar el sistema.

Los virus que infectan archivos, llamados también virus parásitos, se adosan a los archivos ejecutables y son los más comunes. Estos virus pueden esperar a que sean liberados por el usuario al ejecutar el programa, con ello duplicándose rápidamente.

Los virus de macro son un tipo relativamente nuevo, utilizan el hecho de que muchos programas se lanzan con los lenguajes de programación incluidos. Dichos lenguajes están diseñados para ayudar a los usuarios a automatizar tareas mediante la creación de pequeños programas denominados macros. Se dice por ejemplo que los programas de Microsoft Office, se lanzan con un lenguaje interno similar que proporciona muchas macros internas propias.

2.6. EFECTOS DE LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICOS:

Desde su creación los virus informáticos tuvieron un objetivo perfectamente delimitado, causar un daño leve o grave a otros equipos de computación, aunque si recordamos, en sus inicios surgen como un juego y se desarrollaron como una forma de perjudicar a los demás en el aparente anonimato.

Actualmente la creación y propagación de virus informáticos ocasiona serios y devastadores daños, no sólo a los usuarios particulares, sino que también a las economías del mundo, logrando poner en peligro la misma seguridad y la paz mundial. A continuación hablaremos de los efectos de la creación y la propagación de los virus informáticos.

Hemos tratado de abarcar todos los campos o ámbitos en los que consideramos provocan mayores males.

2.6.1. ECONÓMICOS.

La creación y propagación de virus informáticos en la actualidad ha logrado producir serios daños en la economía, no sólo de las personas físicas

quienes comúnmente realizan diversas operaciones bancarias o bursátiles a través del Internet, realizando también diferentes contratos nacionales o transnacionales. También es común que las personas utilicen la red de Internet para comprar algún objeto utilizando su tarjeta de crédito, o para pagar algún servicio. Los virus informáticos también pueden dañar a los sistemas económicos del mundo, los cuales dependen totalmente del uso de computadoras, por lo que de introducirse uno o varios virus se podría causar un colapso económico de gran magnitud, lo cual se traduciría en la perdida de millones de dólares. Afortunadamente, los Estados han podido tomar sus precauciones, sin embargo, viven bajo el temor fundado de que un virus se introduzca en los equipos de cómputo y cause daños. Recordemos que los hackers o piratas están en constante actualización, por lo que los virus sufren constantes adelantos y se sofistican en poco tiempo, lo que significa que sea más difícil el detectarlos e impedir que logren su objetivo. Imaginemos que un virus se activara en las principales bolsas de valores del mundo; los resultados serían catastróficos, en cuestiones de minutos se perderían millones de dólares, y las economías de algunos países se vendrían abajo.

Sin duda el aspecto económico es el de mayor importancia para los países; de hecho, el mundo gira en relación a la economía, por lo cual, los virus informáticos se convierten en una seria y constante amenaza contra todas las naciones, sean del primer mundo o en vías de desarrollo.

2.6.2 POLÍTICOS.

La creación y propagación de virus informáticos tiene también una trascendencia política, puesto que los daños que pueden causar frecuentemente se consideran como actos de los cuales debe responder un país independientemente del autor de los mismos. La comunidad internacional espera que se combata a todo acto que tenga por finalidad crear y propagar algún tipo de virus informático, sancionando a su autor o autores. Por eso es que en algunos países ya existe una policía científica encargada de investigar este tipo de ilícitos y de llevarlos ante los tribunales correspondientes.

Con esto no queremos decir que existe responsabilidad de los Estados cuando uno de sus nacionales crea y propaga un virus informático, al menos desde el punto de vista del Derecho Internacional, aunque si existe una responsabilidad de tipo moral, puesto que hemos señalado que los daños que puede llegar a causar con la propagación de virus informáticos pueden ser verdaderamente desastrosos, sobretodo económicamente para los países. Por esto, hoy es factible saber dónde ha sido creado un virus informático y aunque no constituya aún un delito internacional, el país en el que ha sido creado este microprograma debe encontrar al responsable y sancionarlo tan rápido como le sea posible, dándolo a conocer al mundo.

Por otro lado, la creación y propagación de virus informáticos pueden tener una connotación política internacional de importancia, como una forma de intervención en los asuntos internos de otros países, creando un clima de inestabilidad internacional. Por esto, consideramos que los Estados deben crear caminos de colaboración permanentes en la lucha contra este flagelo moderno que amenaza constantemente nuestro mundo virtual de globalización, donde las economías, las culturas e incluso los sistemas políticos se encuentran entrelazados.

En lo interno, la creación y propagación de virus informáticos también llega a considerarse como un asunto de seguridad nacional, puesto que todo país guarda información confidencial en sus archivos, y un virus puede dañar esa información en cualquier momento, dando por resultado serios daños en lo político y económico. De esta forma, debemos considerar que la creación y propagación de virus informáticos puede llegar a convertirse en un asunto de seguridad nacional.

2.6.3 COMO ACTOS TERRORISTAS.

Por terrorismo podemos entender:

".....la amenaza o uso sistemático de la violencia, tanto por grupos o sectores disidentes organizados, como por fuerzas gubernamentales, oficiales o

no, por lo general los primeros la llevan al cabo de manera abierta y las segundas encubiertamente; contra individuos, organismos, instituciones, integrantes o representativos de gobiernos o grupos políticos, económicos y sociales relevantes específicos, nacionales o extranjeros; con el objeto de lograr la más amplia publicidad posible y sensibilizar a la opinión pública doméstica y mundial acerca de una causa popular para cuya defensa o solución los medios pacíficos han sido inoperantes o se han manifestado infructuosos; o atemorizar e intimidar a la población y reprimir o contener las manifestaciones y reclamaciones populares y el avance de la disidencia política activa".[23]

Tenemos entonces que un acto terrorista es aquél que tiene por finalidad, (como su nombre lo indica), sembrar el terror o causar pánico entre la población, como una forma segura de obtener una meta económica o política. Recordemos los terribles atentados del 11 de Septiembre del año pasado, cuando terroristas afganos impactaron aviones comerciales contra objetivos definidos, causando miles de muertes en la Ciudad de New York y otros más en el Pentagono, etc.

Todo acto terrorista tiene un impacto brutal contra la población que lo sufre e inclusive para aquélla que lo presencia. El terrorismo se ha convertido desde esa fecha en una seria amenaza contra nuestro mundo.

---

[23] Hernández-Vela Salgado, Edmundo. Diccionario de Política Internacional. Editorial Porrúa, S.A. 4ª edición, México, 1996, pp. 535 y 536.

Existen muchas formas de terrorismo, una de ellas muy novedosa es precisamente mediante la creación y propagación de virus informáticos. Si recordamos la creación de ellos, nos daremos cuenta que su utilidad como instrumento para causar terror y daño está probada.

Dijimos ya que constantemente salen a la luz mundial nuevos y más sofisticados virus informáticos que amenazan a millones de usuarios de las computadoras, pero también, se perfilan como actos tendientes a causar desestabilidad económica y política en el mundo. Basta recordar que después de los atentados terroristas del 11 de Septiembre, se siguen recibiendo vía Internet distintas amenazas de grupos fundamentalistas quienes han señalado que destruirán la economía occidental comandada por los Estados Unidos.

El mundo está alerta de otros posibles atentados terroristas y dentro de esa gran preocupación, se espera que se creen y propaguen virus que afecten las comunicaciones y transacciones que diariamente se realizan por medio de las computadoras e Internet.

No hay duda de que estamos ante una nueva forma de terrorismo: el virtual, que puede causar terror en el mundo y muchos daños materiales o económicos. Por eso es importante que la Organización de las Naciones Unidas

emprenda una lucha y constante investigación contra esta forma de terrorismo virtual que podría causar mucho daño a las naciones.

2.6.4. INTERNACIONALES.

Hace algunos años, los virus informáticos eran hechos aislados que no afectaban a los Estados. Sin embargo, en la actualidad, representan un serio problema económico y de seguridad nacional, y es que como lo dijimos, estamos inmersos en un mundo globalizado, interconectado en virtud a la economía, las comunicaciones, la cultura y el comercio. La globalización es un fenómeno que tiene muchas ventajas y desventajas, entre ellas, que los países basan sus relaciones comerciales, económicas, culturales, tecnológicas y políticas en el uso de las computadoras, las cuales les permiten hacer transacciones de cantidades grandes de dinero en cuestión de minutos. Los adelantos cibernéticos como el Internet ha acortado las fronteras entre los países. Por esta razón, México ha celebrado ya numerosos tratados de libre comercio con muchos países o bloques económicos como la Unión Europea.

Reiteramos que el exacto cumplimiento a los compromisos adquiridos por nuestro país depende mucho del uso de las computadoras y el Internet como instrumentos de logística imprescindibles.

Por desgracia, la falta de regulación internacional sobre la creación y propagación de virus coadyuva con aquellos quienes pretenden obtener algún tipo de beneficio económico al realizar los programas computacionales cuya finalidad es causar daño a los servidores de millones de usuarios en todo el mundo.

Finalmente, llamamos la atención en el sentido de que un virus recién creado en un país lejano del nuestro, puede llegar a él en sólo cuestión de minutos, es decir, la creación y propagación de virus informáticos representa un problema mundial que involucra a todos los países y cuya solución debe ser tomada por la comunidad internacional a través de tratados que implementen mecanismos de combate y de colaboración entre ellos para ubicar a quienes crean los virus y los propagan, sancionando esas conductas duramente (mediante las reformas legales internas correspondientes) y así erradicarlos paulatinamente.

2.6.5. SOCIALES.

Nuestra sociedad se ha informatizado, esto significa que las computadoras han entrado en nuestras vidas tomando un lugar especial en ellas.

Como gobernados, tenemos derecho a expresarnos verbalmente o por escrito, de conformidad con los artículos 6º y 7º de la Constitución Política de los Estados Unidos Mexicanos. Esa libertad de expresión debe incluir

necesariamente el uso de la computadoras y de Internet, por tanto, cuando alguien crea y propaga un virus informático, estará causando daños a muchos usuarios, daños que se pueden traducir en pérdidas económicas casi invaluables. Desafortunadamente, la falta de una regulación jurídica adecuada, en muchos países entre ellos México, hace factible que personas sin escrúpulos o que de manera ambiciosa, busquen obtener beneficios económicos jugosos, sembrando el terror entre los usuarios de la red llamada Internet.

Nuestra sociedad necesita tener la seguridad de que podrá usar sus equipos de cómputo y la red de Internet sin que al abrir un archivo se encuentre con la desagradable sorpresa de que está inserto un virus que amenaza con borrar sus demás archivos y la información que se encuentra en ellos.

Es algo incontrovertible que México está aún rezagado en el campo de la investigación y la regulación de los virus informáticos, por eso hace falta que los legisladores tomen conciencia y sobretodo conozcan qué es un virus informático, cómo funciona y cuáles son sus efectos o consecuencias, para estar en posibilidad de crear tipos penales que puedan sancionar estas conductas. Es necesario también que nuestro país cuente con una policía científica especializada en virus informáticos, que pueda fácilmente encontrar a los autores

de virus informáticos y ponerlos a disposición del Ministerio Público, pero también, puedan auxiliar al órgano jurisdiccional que conozca de este tipo de causas penales.

CAPÍTULO 3.

LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICO COMO DELITO EN EL DISTRITO FEDERAL. ALGUNAS CONSIDERACIONES JURÍDICAS.

3.1. LOS DELITOS INFORMÁTICOS Y SU ENTORNO.

Antes de abordar el tema de los llamados delitos "informáticos", el cual es, aún en día, una novedad en nuestro derecho vigente; asimismo, hablaremos brevemente del delito en su aspecto general.

A lo largo del tiempo, los grandes doctrinarios de la materia penal han elaborado diversos conceptos y opiniones sobre el delito, una conducta u omisión que al ser materializada causa daño a otra persona o a la sociedad misma. Así, en términos muy generales, el delito es un acto u omisión que vulnera un deber especificado en la norma jurídica y que el Estado ha impuesto y considerado como obligatorio para todas las personas.

El término "delito" deriva del latín "delinquire", que quiere decir, apartarse del buen camino, alejarse de lo señalado por la ley, etc.

Dentro de los conceptos doctrinales creados por los autores tenemos el del maestro Castellanos Tena, quien dice:

"Como el delito está íntimamente ligado a la manera de ser de cada pueblo y a las necesidades de cada época, los hechos que unas veces han tenido ese carácter, lo han perdido en función de situaciones diversas y al contrario, acciones no delictuosas han sido erigidas en delitos, a pesar de tales dificultades".[24]

El mismo autor cita a otros doctrinarios como Edmund Mezger quien dice del delito:

"El delito es una acción punible, esto es, el conjunto de los presupuestos de la pena". Después, el mismo Mezger dice que el delito es: ".... la acción típicamente antijurídica y culpable".

Eugenio Cuello Calón dice, por su parte:

"Es la acción humana antijurídica, típica, culpable y punible".

[24] Castellanos Tena, Fernando. Lineamientos Elementales de Derecho Penal. Editorial Porrúa S.A. 39ª edición, México, 1998, pp. 128 y 129.

Finalmente, el maestro castellanos Tena cita a don Luis Jiménez de Asúa, el cual señala:

"Delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal".

De las opiniones anteriores de los doctrinarios concluimos que el delito es el acto u omisión típica, antijurídica, culpable y punible por el Estado; es decir, aquello que está prohibido por el mismo Estado y que lesiona intereses de las personas en lo particular y en general de la sociedad.

El artículo 7º del Código Penal Federal (al igual que su homólogo del Código Penal para el Distrito Federal) enuncia que el delito es:

"Delito es el acto u omisión que sancionan las leyes penales".

Los diferentes delitos calificados así por el Estado se encuentran en el código Penal Federal y en los Códigos Penales de cada uno de los Estados de la República, pero también se encuentran tipos penales en otras leyes ya Federales o Locales como el Código Fiscal de la Federación, la Ley Federal de

Armas de Fuego y Explosivos, etc; es decir, son delitos considerados como especiales. A esas leyes se refiere el artículo 7º del Código Penal Federal cuando se refiere a las leyes penales.

Acerca de los delitos informáticos, tema que constituye la esencia de esta investigación, debemos decir que los mismos no existen en la actualidad en nuestra legislación penal, ni local, ni federal vigente; sin embargo, en otras naciones ya son una realidad. Algo similar sucede con el delito de privación ilegal de la libertad en su modalidad de "secuestro express", el cual actualmente, no existe como tal en nuestra legislación; por lo que estas conductas constituyen sólo robos agravados con violencia; sin embargo, a la fecha ya se encuentra en el legislativo del Distrito Federal un proyecto de reforma tendiente a que se tipifique este tipo de ilícitos en los que efectivamente se priva de la libertad (aunque sea por horas) a una persona con el fin de obtener el importe de sus tarjetas de crédito e inclusive, solicitando un rescate a la familia. Es de reconocerse que el legislador del Distrito Federal ya se ha dado cuenta de la trascendencia social y jurídica que tienen estos delitos.

Parecería que el hecho de hablar y hacer un análisis de los delitos informáticos es algo futurista o de ciencia ficción, lo cual resulta totalmente falso. El incremento de la informática y su rol actual en nuestra vida diaria, ha

ocasionado que salga a la luz la necesidad de contar con un marco legal adecuado que le permita al usuario contar con la seguridad jurídica indispensable, que le permita trabajar con ese instrumento imprescindible que hoy en día es la computadora y todo el "software". Bajo este orden de ideas, procederemos a realizar un análisis jurídico de lo que en otros países (tales como, España) son los delitos informáticos y su trascendencia.

Además de los anterior, justifica nuestra investigación el hecho de que nuestra etapa de alta informatización social ha traído también aspectos negativos, como el incremento de la actividad delictiva y la creación de nuevas formas de delinquir, los llamados "delitos de cuello blanco"; grandes fraudes; robos diversos mediante la transferencia de saldos de cuentas bancarias o de tarjetas de crédito, etc. Esto significa que estamos ante una nueva forma de delincuencia, más sofisticada y modernizada, que utiliza sus conocimientos sobre informática para perpetrar sus conductas. Es por lo que resulta necesario e impostergable que nuestros legisladores tomen en consideración estos avances de la delincuencia y también, dinamicen nuestras normas jurídicas penales, tomando como puntos de ejemplo lo realizado en países como España, donde existe incluso, una policía científica especializada en la investigación de los delitos informáticos.

3.1.1. CONCEPTO.

Existen a la fecha algunos estudios doctrinales sobre los delitos informáticos. Tal es el caso del autor Julio Téllez Valdés, autor ya citado en esta investigación y cuyo texto sigue siendo uno de los pioneros en este campo. Este doctrinario e investigador del Derecho Informático nos dice lo siguiente:

"Dar un concepto sobre delitos informáticos no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas; es decir, tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión 'delitos informáticos' esté consignada en los Códigos Penales, lo cual en nuestro país al igual que en otros muchos, no ha sido aún objeto de tipificación; sin embargo y habida cuenta de la urgente necesidad de esto, emplearemos dicha alusión; aunque para efectos de una conceptuación, hagamos el distingo pertinente entre lo típico y lo atípico.

De esta manera tenemos que, dependiendo del caso, 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)".[25]

[25] Téllez Valdés, Julio. Op. Cit. PP. 103 y 104.

En lo particular no notamos diferencia sustancial entre el sentido típico y el atípico a que se refiere el autor, pero sí estamos de acuerdo con él en el sentido de que los delitos informáticos son conductas intrínsecamente delictivas, tipificadas como tales, antijurídicas y que causan daños materiales o patrimoniales a las personas, las cuales se ejecutan a través de la computadora y del conocimiento y uso de software o programas computacionales diversos.

El mismo Julio Téllez Valdés cita a continuación al jurista italiano Carlos Sarzana, quien argumenta que los delitos informáticos son:

"cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".[26]

Para obtener otros conceptos de los delitos informáticos nos remitimos a algunas páginas o "webs" de Internet, ante la escasez de obras jurídico-informáticas publicadas.

Tenemos a la autora Nidia Callegari, quien dice de los delitos informáticos:

"aquel que se da con la ayuda de la informática o de técnicas anexas".[27]

---

[26] Idem.
[27] Vid. www.tiny.uasnet.mx/prof/cln/der/silvis/INDEX.htm.

El autor español Rafael Fernández Calvo dice que el delito informático es:

"... la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1º de la Constitución Española". [28]

La autora y actual Sub procuradora General de la República, la doctora María de la Luz Lima Malvido señala por su parte que delito informático es:

"..... en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que en 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".[29]

La Organización de Cooperación y Desarrollo Económico (OCDE), con sede en Paris, estableció el siguiente concepto: "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de

[28] Vid. www.ctv.es/users/mgp/delitos.html.

[29] Vid. www.colosus.rhon.itam.mx/~sriosma/.

datos y/o transmisiones de datos". La amplitud de este concepto permite englobar las diversas hipótesis de los delitos informáticos, por lo que es, uno de los más completos actualmente.

Finalmente, el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México apunta sobre los delitos informáticos:

"Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".[30]

Más allá de cualquier otra connotación criminológica, los delitos informáticos son, en lo personal, aquellas conductas que tienen por finalidad aprovechar las ventajas que ofrece la informática: hardware y software para obtener alguna ganancia o beneficio económico o político, destruir o causar daños a los ordenadores (computadoras) o a los archivos de otras personas, y que a pesar de no encontrar una tipificación específica en nuestra legislación vigente, en otros países ya son motivo de investigaciones y en su caso, de sanciones penales.

---

[30] Vid. Fundesco.es/seminarios/actas/iosigv.html.

3.1.2. CARACTERÍSTICAS.

El autor mexicano Julio Téllez Valdés se refiere en su obra a las características principales de los delitos informáticos:

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

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

c) Son acciones de oportunidad, en cuanto 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 los realizan.

e) Ofrecen facilidades 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".[31]

Sobre la opinión del autor conviene hacer los siguientes comentarios.

---

[31] Téllez Valdés, Julio. Op. Cit. PP. 104 y 105.

Efectivamente, como ya lo habíamos dicho, los delitos informáticos son considerados como delitos de cuello blanco, en virtud a la forma de perpetrarse, a su dificultad y al resultado obtenido. Son delitos especiales en cuanto a que no cualquier persona puede cometerlos, se requiere de conocimientos técnicos en materia de informática bastante complejos para su realización, por lo que una persona que posea sólo los conocimientos elementales en informática, difícilmente podrá cometer un delito de este tipo.

Diferimos un poco de la opinión del autor, en cuanto a que son delitos "ocupacionales", como él les llama; puesto que, el ánimo delictivo del sujeto pasivo es manifiesto, además, tratándose de acciones como los fraudes a las cuentas bancarias o a las tarjetas de crédito y en la creación y distribución de virus informáticos, se requiere de saber y desear el resultado, por lo que consideramos que sólo excepcionalmente pueden considerarse como delitos ocupacionales, por ello, tampoco estimamos que esencialmente sean culposos o imprudenciales como él los estima. Definitivamente, se trata de delitos dolosos, sonde el sujeto activo sabe y desea el resultado, además, existe un iter criminis o camino del delito en sus dos fases, la interna, de planeación y la externa, de ejecución, independientemente de que se obtenga o no el resultado deseado.

Estos delitos provocan como lo dice el autor, serias pérdidas económicas para los sujetos pasivos y por consecuencia, grandes ganancias para

lo activos. Se pueden llevar a cabo en cualquier computadora, por lo que resultan de fácil realización, incluso hasta para los niños, muchos de los cuales poseen grandes conocimientos sobre informática.

Los delitos informáticos son de difícil comprobación, sobretodo, gracias a la falta de un marco jurídico adecuado. Por lo mismo, son poco denunciados.

3.1.3. CLASIFICACIÓN.

El autor Téllez Valdés, clasifica los delitos informáticos en atención a dos criterios, que son: como instrumentos o medio y como fin u objetivo. En el primer caso, están las conductas criminógenas que utilizan las computadoras como método, medio o símbolo en la comisión del ilícito, ejemplo: la falsificación de documentos mediante el uso del "scanner", como son tarjetas de crédito, cheques, etc.; la variación de los activos y pasivos en la situación de alguna empresa; la planeación o simulación de los delitos convencionales como homicidio, robo, fraude, terrorismo, etc.; el robo de tiempo de computadora; la lectura; sustracción o copiado de información confidencial; la modificación de los datos tanto en la entrada como en la salida; el aprovechamiento indebido o la violación de un código para penetrar un sistema introduciendo instrucciones inapropiadas (lo que se conoce como Caballo de Troya); variación en el destino de

cantidades de dinero hacia una cuenta bancaria apócrifa, lo que se conoce como 'técnica del salami'; uso no autorizado de programas de cómputo; introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios tales como 'consulta a su distribuidor'; alteración en el funcionamiento de los sistemas a través de los virus informáticos; obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos; acceso a áreas informatizadas en forma no autorizada; intervención en las líneas de comunicación de datos o teleproceso.

En la segunda categoría, el autor se refiere a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física, por ejemplo: la programación de instrucciones para producir un bloqueo total en el sistema de uno o varios ordenadores; destrucción de programas por cualquier método; daño a la memoria de la computadora; daño físico a la computadora o sus accesorios (discos, cintas, terminales, etc); sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; secuestros de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago por el rescate, etc.).[32]

La anterior clasificación que hace el doctrinario, resulta altamente ilustrativa, puesto que, nos da un panorama general de todos los resultados que

---

[32] Ibid. P. 106.

se pueden obtener en los delitos informáticos, los cuales pueden agruparse en dos grupos básicos o fundamentales: aquellas conductas en las que se pretende un beneficio económico por parte del sujeto activo, como en los fraudes o robos y aquellos, donde se pretende causar daño material a otras computadoras, ya sea a sus archivos o programas o inclusive al equipo computacional mismo (hardware).

La Organización de las Naciones Unidas ha establecido una clasificación propia de los delitos informáticos, y es la siguiente:

A. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS.

1.- Manipulación de los datos de entrada, conocido también como sustracción de datos, es el delito informático más común, difícil de investigar. En su realización no se requieren grandes y profundos conocimientos técnicos sobre informática.

2.- Manipulación de programas, el cual es difícil de descubrir. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Un método muy usado es el llamado "Caballo de Troya", que consiste en insertar instrucciones en la computadora o servidor de forma encubierta en un programa informático para que pueda realizar

su función no autorizada al mismo tiempo que su función normal, ante la sorpresa del usuario.

3.- Manipulación de datos de salida. Se lleva a cabo fijando un objetivo al funcionamiento del sistema informático. El caso más común es el del fraude que se efectúa a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Antes se utilizaban tarjetas robadas, pero, en la actualidad, se usan equipos y programas computacionales especiales para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

4.- El fraude mediante la manipulación informática en donde se aprovechan las repeticiones automáticas de los procesos de cómputo. Esta técnica se denomina "del salchichón", en la que rodajas muy finas, apenas perceptibles de transacciones financieras, se van sacando de una cuenta y se transfieren a otra.

B. FALSIFICACIONES INFORMÁTICAS.

1.- Como objeto, cuando se alteran los datos de los documentos almacenados en forma computarizada.

2.- Como instrumento, ya que las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial, mediante el uso del "scanner", se pueden lograr reproducciones de alta calidad que muchas veces se confunden con los documentos originales.

C. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COPUTARIZADOS.

1.- Sabotaje informático. Es conocido como el acto de borrar, suprimir o modificar sin autorización, de la funciones o de los datos de la computadora con la intención de obstaculizar el funcionamiento normal del sistema. Dentro de las técnicas utilizadas para este fin están:

1.1.- Virus. Claves programáticas, adheribles a los programas legítimos y se pueden extenderse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, al igual que utilizando el llamado Caballo de Troya.

1.2.- Gusanos. Se fabrican en forma análoga a los virus y se infiltran en los programas informáticos para modificarlos o destruirlos, aunque difieren de los virus en el sentido de que los gusanos no pueden regenerarse. En otras palabras, un gusano es un tumor benigno, mientras que el virus es uno maligno.

1.3.- Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación, o la destrucción o modificación de los datos en un momento dado en el futuro. A diferencia de los anteriores, las bombas lógicas son muy difíciles de detectar antes de que exploten, por lo que poseen un potencial dañino considerable e incomparable. Puede programarse su detonación para que causen el mayor daño posible y ello le da oportunidad al responsable para huir del lugar donde realizó la conducta delictiva. Este mecanismo pude también ser utilizado para solicitar un rescate a cambio de decirle al sujeto pasivo el lugar donde se halla la bomba.

2.- Acceso no autorizado a servicios y sistemas informáticos. Puede ser producido de manera accidental (culposamente) o mediante el pleno conocimiento del acto (dolosamente), como sucede con los piratas electrónicos o "hackers" profesionales en este tipo de conductas delictivas, hasta en el espionaje o sabotaje informático. Este tipo de delincuentes aprovecha la falta de una regulación jurídica adecuada para realizar sus actos ilícitos. Frecuentemente, los "hackers" o piratas informáticos se hacen pasar por usuarios legítimos del sistema con la detección de las contraseñas o "passwords" que poseen aquellos.

3.- Reproducción no autorizada de programas informáticos de protección legal, es decir, los conocidos actos de piratería, la que ha incursionado rápidamente en los programas computacionales. Es así que resulta fácil y barato

el encontrar clandestinamente un programa novedoso que en su precio normal estriba en doscientas o más veces el del artículo pirata. Recordemos que todos lo programas computacionales, al igual que las obras literarias, artísticas y científicas gozan de protección legal siempre cuando estén registradas en el Organismo llamado Registro del Derecho de Autor, dependiente de la Secretaría de Educación Pública. La reproducción ilegal de los programas informáticos constituye un delito Federal y es uno de los problemas más graves desde el punto de vista del detrimento económico que traen para el o los titulares de esos derechos.

Podemos agregar a la lista de la ONU, los siguientes delitos informáticos, para mayor abundamiento en el tema:

1.- Acceso no autorizado de contraseñas o passwords y la entrada a un sistema informático sin la autorización del titular.

2.- Destrucción de datos. Daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

3.- Infracción al "copyright" de la base de datos. Uso no autorizado de información almacenada en una base de datos.

4.- Intercepción de correos electrónicos o "e-mails" y su lectura sin la autorización del titular.

5.- Transferencias de fondos bancarios de una cuenta a otra.

En la red de redes o Internet, se pueden realizar los siguientes delitos:

1.- Espionaje. Acceso no autorizado a los sistemas informáticos gubernamentales y de grandes empresas y de correos electrónicos.

2.- Terrorismo, mediante la propagación de mensajes anónimos por grupos, cuyo objetivo es sembrar el miedo entre la población.

3.- Narcotráfico, mediante la transmisión de fórmulas para la fabricación de estupefacientes, lavado de dinero y otras actividades conexas.

4.- La red puede ser utilizada para cometer otros delitos como el tráfico de armas, el proselitismo de sectas o de grupos extremistas, etc.

3.1.4. ORGANISMOS DE PREVENCIÓN EN OTROS PAÍSES.

La aparición de los delitos informáticos ha dado pauta a que países preocupados por los daños que tales conductas causan, emprendieran una cruzada frontal contra ellos. Así es como han creado una estructura jurídica básica que permite investigar y en su caso, sancionar estos ilícitos, pero también se han tenido que crear organismos gubernamentales especializados en la investigación y la prevención de los delitos materia de esta investigación.*

Naciones como España han llegado a crear una policía científica y especializada en la investigación de los delitos informáticos. Inclusive en ese país han llegado a restringir el acceso a las páginas pornográficas en los cafés Internet, sancionándolos en caso de incumplimiento; medida que estimamos exagerada, pero que nos da un ejemplo de la preocupación que España tiene sobre el mal uso de la informática.

Cabe agregar que Venezuela cuenta ya con una ley específica llamada: "Ley Especial Contra Delitos Informáticos", publicada en la Gaceta Oficial número 37.313 de fecha 30 de octubre de 2001, en cuyo artículo 1º dice que. "La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos

* Ver Apéndice: caso Hipahack, sentencia española.

cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley".

En cuanto a los organismos en el mundo que se dedican a la búsqueda, reducción, eliminación y prevención de los delitos informáticos tenemos a la Guardia Civil Española, pionera en la investigación de esta clase de delitos. Los guardianes españoles tienen especial colaboración con otras policías en el mundo, principalmente con las europeas como la Scotland Yard, el F.B.I. (Federal Bureau of Investigation), la P.A.F. de Francia, etc.

En los Estados Unidos de América existen agentes especializados en la investigación de estos ilícitos, aunque también, es en ese país donde se producen muchos ilícitos informáticos.

En Argentina, la División de Computación de la Policía Federal, conformada por doce efectivos y a cargo del subcomisario Alberto Airaia, están patrullando constantemente la red en busca de delitos informáticos. Algunas veces lo hacen oficiosamente y otras a petición de la autoridad judicial.

En Buenos Aires existe un importante grupo: el de Investigación en Seguridad y Virus Informáticos (G.I.S.V.I.), creado en la Universidad de Buenos Aires en 1995, actualmente también funciona en la Universidad de Belgrano. Este

grupo ha podido resolver ya algunos casos de ataques de virus a empresas cuyas características son de actos de sabotaje informático. Desafortunadamente, la difícil situación que atraviesa Argentina puede perjudicar los avances que ese país del sur del Continente han alcanzado. Estos organismos son sólo ejemplos de una preocupación latente que los Estados han manifestado por perseguir y sancionar los delitos informáticos. Sirven de ejemplo también para nuestros legisladores a efecto de que México cuente con una policía científica encargada de la investigación y persecución de estas conductas que son consideradas por ellos como novedosas o cosas de ficción.

3.1.5. LA CALIDAD DE LOS SUJETOS ACTIVOS Y PASIVOS.

De lo que hemos hablado anteriormente se desprende que los sujetos que intervienen en la comisión de los delitos informáticos son: los activos; es decir, quienes realizan la conducta delictiva, son específicos o especiales, puesto que, se requiere que tengan conocimientos profundos sobre informática, especialmente sobre software, programas y archivos computacionales, independientemente de la edad que tengan. Los sujetos activos requieren una computación equipada con los programas básicos como windows en su versión 98 o 2000 y sobre todo con Internet. Por esto se dice que se trata de delincuentes de cuello blanco, quienes no se manchan las manos con la conducta, sino que en

la comodidad de su hogar, oficina u otro lugar pueden llevar a cabo el delito. Reiteramos que los sujetos activos de este tipo de delitos poseen un nivel intelectual muy amplio para poder meditar la forma de llevarlos a cabo.

Los sujetos pasivos pueden ser cualquier persona, pero, se requiere que tengan conocimientos sobre informática también, aunque estos no sean tan profundos como los activos. Esta calidad especial implica que el sujeto sepa usar la red de redes llamada Internet y que realicen operaciones bancarias o de algún otro tipo en donde manejen fondos propios o ajenos de dinero, o que simplemente utilicen la computadora y sus programas como forma de realizar sus labores diarias. De esta manera, una ama de casa, un estudiante o cualquiera otra persona que utilice la computadora y el software para cualquier finalidad, puede ser víctima de un virus informáticos que dañe sus programas o archivos, incluso, que le ocasione daños severos a su equipo de computación.

3.1.6. DERECHO COMPARADO.

En este apartado mencionaremos brevemente los cuerpos jurídicos existentes en otros países tendientes a regular y sancionar los delitos informáticos.

Ya hemos mencionado que Venezuela cuenta con una ley especial destinada a regular este tipo de ilícitos y sancionarlos, de fecha 30 de octubre del 2001.

Argentina cuenta con una Policía Federal especializada en la investigación de los delitos informáticos; así como en los constantes estudios en esa materia en la Universidad de Buenos Aires, como ya fue explicado con anterioridad.

En Alemania, se adoptó en fecha 15 de mayo de 1986, la segunda Ley contra la Criminalidad Económica, en la cual se contemplan el espionaje de datos, la estafa informática, la falsificación de datos probatorios, de documentos, la falsedad ideológica, la alteración de datos, la utilización abusiva de cheques o tarjetas de crédito, etc.

En Austria, la reforma legal al Código Penal Federal de fecha 22 de diciembre de 1987 adiciona los delitos de destrucción de datos, tanto los personales como los no personales y los programas computacionales; la estafa informática, cuya hipótesis se refiere a aquellos que dolosamente causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos a través de la confección de un programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

Se contemplan también sanciones para quienes cometen este hecho a sabiendas de su profesión; es decir, se agravan las sanciones.

En Francia, la Ley número 88-19 del 5 de enero de 1988, relativo al fraude informático, regula subtipos penales como el acceso fraudulento a un sistema de elaboración de datos; el sabotaje informático; la destrucción de datos; la falsificación de documentos informatizados y el uso de documentos informatizados falsos.

En gran Bretaña, gracias a un caso de "hacking", en 1991 comenzó a regir la Ley de Abusos Informáticos o "Computer Misuse Act". Dentro de sus contenidos se dispone que el intento, acabado o no de alterar datos informáticos se sanciona con una pena hasta de cinco años de prisión.

En Holanda, en fecha 1º de marzo de 1993 entró en vigor la Ley de Delitos Informáticos, en la que se penaliza el hacking, el "preacking" (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (conocido como el arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus, conducta sancionada de diferente forma si se causa dolosamente o culposamente. En el primer caso, la pena puede llegar hasta los cuatro años de prisión, mientras que en el segundo caso apenas puede llegar al mes de prisión.

En España, el nuevo Código Penal, en su artículo 263 dispone que se impondrá sanción a quien cause daños en propiedad ajena. El artículo 264-2 establece que se aplicará 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 Código en comento sanciona también la divulgación de secretos, el espionaje y la divulgación de secretos, así como la estafa con ánimo de lucro valiéndose de cualquier manipulación electrónica.

Chile fue el primer país latinoamericano en sancionar los delitos informáticos, para ello, cuenta con su Ley contra Delitos Informáticos, la cual entró en vigor en fecha 7 de junio de 1993. Dentro de los aspectos destacables de ese cuerpo normativo están que la destrucción o inutilización de los datos contenidos dentro de una computadora se sanciona con penas que van desde un año y medio hasta cinco años de prisión. Dentro de esas hipótesis se incluyen también a los virus informáticos.

Los Estados Unidos de América han mostrado interés por el incremento de los delitos informáticos, por lo que han introducido en su legislación

algunas novedades tendientes al combate de estos delitos que bien sabemos, tienen su origen en ese país.

Entre otras medidas legales, en el año de 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), la cual modificó el acta de Abuso Computacional de 1986. Esta Ley sanciona la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, al sistema informático, a las redes, a la información, datos o programas. Podemos decir que esta ley es novedosa puesto que sanciona los actos de transmisión de virus informáticos. Esta Ley considera que la creación y propagación de virus informáticos puede ser de dos maneras: intencionalmente o dolosamente y accidentalmente o culposamente. En el primer caso, la sanción es hasta de diez años (es un delito federal), más una multa, y en el segundo caso, la pena fluctúa entre una multa y un mes de prisión.

La Ley en comento, constituye un gran avance no sólo en el territorio de los Estados Unidos, sino que es un ejemplo para el mundo, por que los Estados Unidos llevan la delantera en materia de combate a los delitos informáticos.

En materia local, en el Estado de California, en 1992, se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos, aunque en

menor grado que en la Ley anterior. Se modificó el Código Penal de ese mismo Estado a efecto de ampliarse las sanciones económicas (multas a quienes creen y/o propaguen virus informáticos). Estas sanciones tienen por objeto resarcir el grave daño patrimonial que este tipo de delitos les causa.

En el Tratado de libre Comercio (T.L.C. o NAFTA), los tres Estados partes de ese instrumento que entró en vigor en 1994 estipularon su compromiso por la defensa de los derechos de autor y los llamados conexos. Dentro de los primeros se incluyen también a los programas de computo, debiendo cada Estado tomar las medidas legales oportunas y necesarias para sancionar cualquier acto que viole este importante derecho que asegura la creación intelectual (artículo 1714). El artículo 1711 se refiere a la protección de los secretos industriales y de negocios, impidiendo que estos sean revelados sin derecho. Desafortunadamente, en el caso de México, sobre todo el incremento de la piratería de los programas computacionales, no ha podido ser detenido y con ello las pérdidas de las empresas en ese ramo han sido multimillonarias.

La actual Ley Federal del Derecho de Autor del 24 de diciembre de 1996 y que entró en vigor al año siguiente establece un marco legal adecuado para la protección de los programas de computo y del derecho de sus creadores.

Toda vez que la Ley era omisa en materia de delitos en el campo del

derecho de autor, se propuso conjuntamente una reforma y adición al Código Penal (del Distrito Federal y Federal supletoriamente), reformas que habrían de inhibir y sancionar la práctica de conductas violatorias del derecho de autor y de los derechos conexos. Así, actualmente, el Código Penal Federal en su Título Noveno, Capítulo segundo se refiere al "acceso ilícito a sistemas y equipos de informática", con disposiciones que comentaremos después y que complementan a la Ley Federal del derecho de Autor.

Cabe agregar que el Código Penal para el Estado de Sinaloa es novedoso en el sentido que tutela los delitos informáticos en su artículo 217 en estos términos:

"Comete delito informático, la persona que dolosamente y sin derecho:

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

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

Es interesante y visionario este numeral puesto que regula de una manera muy general los delitos informáticos, tutelando el patrimonio de los usuarios de computadoras y de softwares; toda vez que, estos ilícitos atentan y lesionan seriamente el citado patrimonio de las personas. El artículo en cuestión se refiere también a la creación y propagación de virus informáticos. Las sanciones son realmente menores: prisión de seis meses a dos años y una multa de noventa a trescientos días multa. Otro aspecto digno de destacarse es que el artículo no acepta la culpa como forma de comisión. Es un delito totalmente doloso, lo cual nos parece exagerado, pues sí creemos que se pueda cometer de forma culposa, por negligencia o error, sin el ánimo de causar daño.

3.2. NECESIDAD DE CREACIÓN DE UN TIPO PENAL EN MATERIA DE CREACIÓN Y PROPAGACIÓN DE UN VIRUS INFORMÁTICO.

Los delitos informáticos son algo nuevo en la mayoría de las legislaciones de los Estados de la República mexicana, a excepción de Sinaloa, en cuyo Código Penal sí se contemplan esos ilícitos y del Código Penal Federal en cuyo Titulo Noveno, Capítulo Segundo se regulan y sancionan los delitos informáticos, aunque no sea muy contundente esa regulación, puesto que de la

lectura de los artículos que integran ese Capítulo, artículos 211-bis 1 al 211-bis 7, no se desprende regulación alguna de la creación y propagación de virus informáticos como una conducta delictiva; sin embargo, estos artículos constituyen un gran avance en nuestro derecho, pues, finalmente el legislador se dio cuenta de la necesidad e importancia de perseguir y sancionar conductas que tengan por finalidad obtener un beneficio económico o simplemente causar un daño a otros equipos de computo mediante la creación y la propagación de virus informáticos.

La regulación de los delitos informáticos es a la fecha materia federal (ante la falta de una regulación local más específica), por lo que le corresponde investigar esos delitos a la Procuraduría General de la República.

Consideramos que es momento oportuno de que el Distrito Federal, asiento de los Poderes Federales y capital del país, ciudad con más de veinte millones de personas cuente con una regulación penal de los delitos informáticos, incluyendo la creación y propagación de virus; y así estar en condiciones de combatir este tipo de ilícitos denominados de cuello blanco que causan daños serios a los sujetos pasivos en sus patrimonios, y que además pueden ser instrumentos muy útiles para el desarrollo del terrorismo no sólo en México, sino en todo el mundo.

3.2.1. JUSTIFICACIÓN JURÍDICA, ECONÓMICA Y SOCIAL.

Le existencia en la Ley sustantiva penal de un tipo determinado obedece necesariamente a una "ratio legis"; es decir, a razones de índole jurídico, social e inclusive, económico. Tal es el caso de los delitos informáticos, los cuales inciden en un detrimento serio de nuestra sociedad y de la economía o patrimonio de muchas personas físicas o morales, quienes utilizan las computadoras y diferentes programas o software para realizar movimientos bancarios o en la Bolsa y quienes de la noche a la mañana, descubren con gran asombro que sus fondos han sido vaciados sin explicación alguna por parte de las instituciones bancarias y de crédito o la misma Bolsa de Valores. En el menor de los casos, personas comunes quienes realizan sus actividades laborales utilizando una computadora y sus programas respectivos reciben un correo electrónico en el que va incrustado un virus el cual al ser abierto, permitirá al virus causar daños en los archivos, programas o inclusive, en el disco duro de la computadora, produciendo un detrimento material y económico de consideración, el cual para una persona quien depende de su equipo de cómputo y de sus programas representa una acto que pone en peligro su sobre vivencia y la de su familia.

El Distrito Federal es la ciudad más poblada del mundo con más de veinte millones de personas actualmente; y siguen llegando a ella otras más con

el propósito de establecerse y encontrar mejores condiciones de vida. Por esta razón, los problemas que existen en ella se han multiplicado, rebasando los mecanismos de solución y los planes y programas de la autoridades. Así, problemas como la falta de vivienda, la falta de trabajos bien remunerados, la corrupción cada vez más marcada, los problemas ambientales graves, la explosión demográfica señalada y sobre todo, el nivel de inseguridad pública que priva en esta ciudad, con el incremento de los delitos respectivo.

La falta de un Estado de Derecho donde todo ilícito se sancione ha dado pauta para la proliferación de delitos como el robo con violencia, la privación ilegal de la libertad y su modalidad de secuestro express, los homicidios, y sobre todo, los delitos de cuello blanco, dentro de los que se cuentan los delitos informáticos.

Por otro lado, el avance en el estudio y manejo de las computadoras y de sus programas, aunado a la publicidad de los medios de comunicación han propiciado que los delincuentes busquen y encuentren otros campos fértiles para llevar a cabo sus actividades delictivas. De esta manera, personas quienes cuentan con extensos conocimientos en computación descubren que es relativamente fácil el transferir una cuenta bancaria a otra, crear un virus y causar daño a los equipos computacionales de otras personas, etc. Indudablemente que en el clima de inseguridad pública en que se vive en esta ciudad, donde

esperamos seguir vivos el día siguiente, lo menos que nos llega a interesar a los ciudadanos y a la autoridad es la comisión de delitos informáticos; sin embargo, para aquellas personas quienes sufren un robo en su cuenta bancaria o en su tarjeta de crédito, ese acto es de graves consecuencias para su patrimonio. Además, si aspiramos como sociedad a contar con un clima de seguridad pública donde reine el imperio de la norma jurídica, debemos entender que todos los delitos deben ser investigados y sancionados, pues, independientemente de que se trate de delitos graves o no, todo delito es un acto que lesiona a la sociedad mexicana.

Hemos dicho también que la etapa de avances cibernéticos que estamos experimentando ha sido también de beneficio para los delincuentes, los cuales se han sofisticado en sus modus operandi. Es así que una banda de secuestradores o de narcotraficantes cuentan con un buen equipo de cómputo para realizar sus actividades. En este mismo tenor de ideas, los delitos informáticos le pueden aportar a los delincuentes grandes ganancias utilizando un equipo de computación propio o rentado. Tengamos presente que en los últimos tres años han proliferado los llamados "cafés Internet", donde una persona renta una computadora por el tiempo que estime necesario y en ella puede realizar delitos informáticos tranquilamente, puesto que al no haber regulación especial, el café Internet no se hace responsable de las actividades que realicen sus clientes.

Por estas razones, estimamos que resulta necesario que el Código Penal para el Distrito Federal cuente con un tipo penal, por lo menos, que regule y sancione los delitos informáticos y en especial, la creación y propagación de virus.

3.2.2. PROPUESTA DE ADICIÓN AL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, QUE REGULE Y SANCIONE LA CREACIÓN Y PROPAGACIÓN DE UN VIRUS INFORMÁTICO CON EL ÁNIMO DE CAUSAR DAÑO A LOS USUARIOS DE LA RED INFORMÁTICA.

Creo que este trabajo de investigación no estaría completo, si careciera de algunas propuestas legales que ayuden a enfrentar el problema de los delitos informáticos y que sembraran en el legislador la inquietud o curiosidad de conocer más de ellos y de su trascendencia en el México actual de cambios y avances tecnológicos.

Una de las propuestas es la de adición al Código Penal para el Distrito Federal de un precepto que se complemente con el Título Noveno, Capítulo Segundo del Código Penal Federal y que sancione la creación y propagación de virus informáticos, ya que este tipo de delito informático no se desprende de la lectura de los artículos de la Ley Penal sustantiva federal. Antes

de mostrar la propuesta de adición al Código Penal para el Distrito Federal, resulta conveniente remitirnos al Código Penal Federal:

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

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

Este numeral se refiere al acto de modificar, destruir o provocar la pérdida de información que obre en sistemas o equipos informáticos que estén protegidos por algún mecanismo de seguridad, en cuyo caso, la pena es de seis meses a dos años de prisión y una multa de cien a trescientos días de salario mínimo vigente. En la segunda hipótesis, el artículo habla de que se sancionará a quien copie información contenida en sistemas o equipos de informática con una pena que va de los seis meses a un año de prisión y una multa de cien a ciento cincuenta días de salario mínimo vigente en el Distrito Federal. El artículo no hace referencia al modus operandi o forma de realizar esos actos, por lo que tampoco se refiere a la creación y propagación de virus informáticos.

Los artículos 211-bis 2 y 3, hacen referencia al Estado mexicano como sujeto pasivo del delito mencionados en el numeral anterior. Tampoco se habla de la creación y propagación de virus informáticos. Los artículos 211-bis 4 y 5, versan sobre las instituciones financieras como sujeto pasivo del delito. En todos los artículos mencionados se encuentra la misma redacción, por lo que estimamos que este Capítulo no representa un marco legal apropiado para el combate a los delitos informáticos y en especial, a la creación y propagación de virus.

Tomando en consideración lo anterior y sobre todo, el gran paso que el Estado de Sinaloa ha dado en este campo es que proponemos que el Código Penal para el Distrito Federal cuente con un apartado especial para el combate de los delitos informáticos en general y en especial, de la creación y propagación de virus informáticos, tema esencial de esta investigación.

La creación de un tipo penal representa una labor muy delicada y ardua, por lo que sabedores de la responsabilidad que ello implica, creemos que debe adicionarse al Código Penal para el Distrito Federal un segundo Capítulo en su Título Noveno (al igual que sucede en el Código Federal), relativo a los Delitos Informáticos", en este sentido:

TÍTULO NOVENO.

REVELACIÓN DE SECRETOS.

CAPÍTULO I.

.....

.....

.....

CAPÍTULO 2.

LOS DELITOS INFORMÁTICOS.

Artículo 211-bis 1. Comete delito informático, la persona que obrando dolosa o culposamente y sin derecho y utilizando equipos de cómputo propios o ajenos, cause un daño patrimonial a los usuarios de otros equipos de computación u obtenga un beneficio económico indebido mediante la creación, propagación, intercepción, alteración o destrucción de los programas de cómputo de una o varias personas".

"Artículo 211-bis 2. Al que a sabiendas de la consecuencias que ello produce, cree o propague programas computacionales o "virus informáticos", mediante el uso de Internet, a otros equipos de cómputo, públicos o privados, se le aplicará una pena de seis meses a dos años de prisión y una multa de cien a quinientos días de salario mínimo en el Distrito Federal".

"Artículo 211-bis 3. A los que reincidan en la creación o en la propagación de virus informáticos se les aplicará una pena de dos a cinco años y una multa de quinientos a mil días de salario mínimo vigente en el Distrito Federal".

Estimamos que la definición de delito informático en general que ofrecemos en el artículo 211-bis 1, es bastante general y entendible para cualquier persona, además de que resulta muy necesaria. En el siguiente artículo, nos referimos al delito de creación y propagación de virus informático, imponiéndole una sanción de seis meses a dos años de prisión y una multa de los cien a los quinientos días de salario mínimo vigente en el Distrito Federal.

En al artículo 211-bis 3, que proponemos, se habla de la reincidencia en la que pueden caer fácilmente quienes han creado o propagado un virus informático y saben de sus consecuencias. En este caso, la pena se aumenta de los dos a los cinco años de prisión y una multa de los quinientos a los mil días de salario mínimo vigente en el Distrito Federal.

3.3. NECESIDAD DE CONTAR CON UNA POLICÍA CIENTÍFICA CAPACITADA PARA INVESTIGAR LA CREACIÓN Y PROPAGACIÓN DE VIRUS INFORMÁTICO.

Además de las adiciones propuestas al Código Penal para el Distrito Federal ya explicadas, consideramos que nuestro país necesita contar con una policía especializada en la investigación y detección de delitos informáticos, especialmente, en la creación y propagación de los mismos.

Sabemos que el hecho de proponer la existencia de una nueva policía, sea federal, local o municipal representa la erogación de mucho dinero, en una época en la que el presupuesto destinado a la seguridad pública ha experimentado como en otros rubros, un deceso importante. Sin embargo, tenemos como soporte de esto, el hecho de que ya existe dentro de la Policía Federal Preventiva una unidad "cibernética", dedicada a conformar el primer banco de datos de bandas delictivas mexicanas que realizan tráfico de prostitución infantil y que utilizan el Internet para estos fines. Para ello, esta novel "Policía Cibernética" ha realizado ya, constantes patrullajes anti hackers en el ciberespacio. Uno de los resultados más importantes obtenidos a la fecha, es haber descubierto en Guerrero una de las bandas más importante a nivel mundial dedicada a la pedofília, encabezada por un ciudadano de los Estados Unidos, Robert Decker, detenido y expulsado de México hacia su país de origen, donde ya

contaba con una orden de aprehensión por el mismo delito. Observamos que esta unidad "cibernética", tiene una función limitada actualmente, sin embargo, creemos que en un tiempo razonable, obtendrá mayores atribuciones legales que le permitan investigar y prevenir otros ilícitos que se llevan a cabo en el ciberespacio, tales como, los delitos informáticos y especialmente, la creación y propagación de virus.

Así mismo, proponemos que otros cuerpos policíacos como la nueva Agencia Federal de Investigación (antes Policía Judicial Federal), también sean capacitados en aspectos técnicos profundos de las computadoras y de sus programas, incluyendo Internet. Además, son necesarios cursos de idiomas (inglés por lo menos), de contabilidad y de cultura general que les permita entender a los diversos delincuentes de cuello blanco y su modus operandi.

La existencia de estos grupos especiales en la investigación y en el combate a los delitos informáticos debe basarse en los éxitos obtenidos por otras naciones que ya cuentan con ellos. Creemos que sólo de esta manera nuestro país podrá contar con una mejor detección y disminución de los delitos informáticos y así, salvaguardar el patrimonio de muchas personas quienes usan las computadoras para sus labores y transacciones diarias, lo que se traducirá en un paso más hacia el reestablecimiento de nuestro Estado de Derecho y por ende, de la seguridad pública.

En el establecimiento de estos grupos policíacos, deben trabajar unidos los gobiernos Federal, Locales y municipales, así como colaborar con los gobiernos e instituciones extranjeras como el F.B.I. o la INTERPOL, ya que de esta manera se podrá establecer un mecanismo de combate y sanción a los delitos informáticos y sus letales consecuencias, un mal de nuestra modernidad y de una época revolucionada y carente de muchos valores morales.

CONCLUSIONES.

Primera.- Las computadoras constituyen uno de los inventos más extraordinarios que el hombre ha podido llevar a cabo. Su uso le ha permitido realizar múltiples tareas en menos tiempo y con ahorro de recursos humanos y económicos. En la actualidad, nuestra vida gira en torno a las computadoras, por lo que podemos señalar que vivimos inmersos en una etapa informatizada.

Segunda.- El avance de las computadoras desde las décadas de finales de los treintas y los cuarentas a la fecha ha sido vertiginoso y casi de ciencia ficción. Hoy contamos con computadoras disponibles para cada necesidad y cada bolsillo, con muchos programas computacionales o "software", que nos permite hacer nuestras tareas con suma facilidad, aún las más complicadas e inclusive Internet, una gran red de redes interconectadas entre sí que permite el flujo e intercambio de la información en cuestión de segundos, sin importar las distancias.

Tercera.- Uno de los términos más utilizados en el mundo de las computadoras es el de "informática", por éste debemos entender a la disciplina compuesta por un conglomerado o conjunto de técnicas utilizadas para

sistematizar de forma lógica y automática cualquier tipo de información la cual habrá de ser utilizada por el interesado en la toma de decisiones que corresponda.

Cuarta.- El desarrollo vertiginoso de la informática ha traído como consecuencia, la existencia de muchos tipos de programas, diseñados para ayudar al hombre en sus labores diarias. Desde la ama de casa o el estudiante hasta el gran empresario cuyas necesidades de sistematización son muy exigentes, se han visto beneficiados con los programas computacionales o "software" disponibles en la actualidad. Sin embargo, este gran avance en materia de informática ha dado pauta a la creación y propagación de algunos programas de cómputo cuyo objetivo puede ser benigno o maligno, causando daño en los archivos, programas e inclusive en el llamado "disco duro" de la computadora, mecanismos o programas que se han denominado: "virus informáticos", los cuales han encontrado la vía idónea para su multiplicación y acceso a los equipos de miles de usuarios de computadoras a través del Internet.

Quinta.- Los virus informáticos son programas de cómputo diseñados para causar daño en los archivos, programas o en el equipo mismo del usuario. Pueden multiplicarse rápidamente e inclusive, pasar inadvertidos por el usuario hasta el momento en que el mismo abre un archivo nuevo y permite salir al virus el cual infectará los demás archivos, programas o el equipo mismo,

cumpliendo así, su cometido. El daño patrimonial que causan los virus informáticos puede ser de mucho dinero, según sea la parte del equipo que resulte afectada. Recordemos que virus como el "Anna Kournikova", el "I love you", código rojo, etcétera. rápidamente se propagaron en el mundo afectando a miles de usuarios en Internet, quienes los recibieron.

Sexta.- El origen de los virus informáticos se remonta a los años sesentas cuando varios estadounidenses que laboraban en la empresa Laboratorios Bell de AT & T crearon un programa de cómputo como una forma de diversión llamado "Core War", en el "core" o memoria de la computadora. Dicho programa se prohibió por considerarse como peligroso al elaborarse otros mini programas destinados a forzar al ordenador del oponente a cumplir una acción válida, ganando quien lo consiguiera primero. Este juego se comenzó a realizar en forma clandestina difundiéndose rápidamente en el mundo.

Séptima.- Se han realizado estudios sobre los virus informáticos encontrándose gran diversidad de ellos. Entre los más importantes están: las bombas, los camaleones, los reproductores, los gusanos y los llamados Caballos de Troya. Cada uno de ellos tiene una función especial una vez que se encuentran en el interior del ordenador o computadora.

Octava.- Los virus informáticos se han convertido en pocos años en una verdadera pesadilla y psicosis para los usuarios quienes viven con el temor de que reciban un mensaje en el que esté incrustado un virus que pueda producir severos daños en su equipo archivos o programas.

Novena.- Los virus informáticos son creaciones de personas con amplios conocimientos de computación, cuyo objetivo es causar daños serios o graves en los equipos de otras personas y con ello, un detrimento patrimonial considerable.

Décima.- Los virus informáticos pueden propagarse a través del Internet (siendo la vía idónea, ya que en cuestión de minutos pueden llegar a miles de personas en todo el mundo), pero también, por medio de diskettes contaminados.

Décimo primera.- Los virus informáticos tienen actualmente un importante entorno social, político, de seguridad pública e internacional y sobre todo económico, ya que el daño que pueden causar es enorme, como ya ha quedado explicado en el cuerpo de esta investigación.

Décimo segunda.- A diferencia de otros países en los que su legislación penal sustantiva contempla y sanciona los llamados delitos informáticos, en la nuestra existe apenas una mención en el Código Penal Federal, en sus artículos 211-bis del 1 al 7, en su Título Noveno, Capítulo Segundo, relativo al acceso ilícito a sistemas y equipos de informática, aunque el espíritu de esos artículos es fundamentalmente el tutelar la información estatal y de las instituciones bancarias y de crédito, por lo que otros delitos informáticos como la creación y propagación de virus informáticos son también casi inexistentes a excepción del Código Penal del Estado de Sinaloa en cuyo artículo 217 se sanciona el acto de usar o entrar a una base de datos, sistemas o red de computadoras o a cualquier parte de ella, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información, o intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computación o los datos contenidos en ella, en la base, sistema o red. Esta redacción es un avance significativo en la regulación de los delitos informáticos en nuestro derecho vigente.

Decimotercera- Los delitos informáticos son aquellas conductas ilícitas que se realizan con la ayuda de las computadoras y de algunos programas o software con el propósito de obtener algún beneficio económico o simplemente, causar un daño en los archivos, programas o en el equipo computacional de uno o varios usuarios.

Decimocuarta.- Los delitos informáticos son considerados como delitos de cuello blanco, puesto que para su realización se requieren conocimientos técnicos especiales (calidades especiales en los sujetos) y sólo se requiere un equipo de cómputo propio o ajeno para llevarlos a cabo.

Decimoquinta.- En otros países como Alemania, Austria, Argentina, Francia, Gran Bretaña, Holanda, España, Estados Unidos, Chile y Venezuela, existe ya un marco legal vigente sobre los delitos informáticos, por lo que nuestro país no puede quedarse rezagado, y menos aún cuando se ha comprometido en virtud del Tratado de Libre Comercio a proteger los derechos de autor de quienes crean programas de cómputo.

Decimosexta.- Por estas razones y dada la gravedad que representa la creación y propagación de virus informáticos, proponemos algunas medidas que estimamos sean factibles y que coadyuven al combate de este tipo de delincuencia llamada de cuello blanco. Las medidas son:

a) La adición de un artículo al Código Penal del Distrito Federal que regule la creación y la propagación de virus informáticos, en los términos descritos y explicados en el Capítulo Tercero de esta investigación;

b) El establecimiento formal y el desarrollo de una policía científica o cibernética, (que de hecho ya existe como una atribución de la Policía Federal

Preventiva en los delitos de secuestro, narcotráfico, etcétera), en cada uno de los Estados de la Federación mexicana;

c) La necesaria capacitación y actualización permanente de los cuerpos policíacos encargados de investigar los delitos informáticos en materias como: computación en sus programas fundamentales como windows, excel, power, point, outlook, sobre todo, en Internet. Además, en Inglés, Contabilidad, Derecho, etcétera.

d) La fiscalización constante y adecuada de los cafés Internet que se han multiplicado en ciudades importantes como el Distrito Federal, pues el usuario puede crear ahí y propagar los virus informáticos, así como otro tipo de delitos de este tipo y fomentarse así otras conductas como la pornografía infantil, ya que no existe un control en esos centros de renta de computadoras.

e) Difundir las distintas Procuradurías tanto Locales, como la General de la República en coordinación con otras instancias como la Secretaría de Seguridad Pública Federal, las consecuencias que traen consigo los virus informáticos y la importancia de que los usuarios de computadoras y sobre todo de Internet, estén capacitados y sean cuidadosas de los mensajes o archivos que reciben de forma misteriosa.

BIBLIOGRAFÍA.

BURGOA ORIHUELA, Ignacio. Derecho Constitucional. Editorial Porrúa, S.A., octava edición. México, 1991.

CASTELLANOS TENA, Fernando. Lineamientos Elementales del Derecho Penal. Editorial Porrúa, S.A., 39ª edición, México 1998.

DE LA CUEVA, Mario. El Sistema UNAM-JURE, Un Banco de Datos Legislativos. UNAM, México, 1985.

GARCÌA MAYNEZ, Eduardo. Introducción al Estudio del Derecho. Editorial Porrúa, S.A., 49ª edición, México, 1998.

HANCE, Olivier. Leyes y Negocios en Internet. Editorial Mc Graw Hill, México, 1997.

HERNÁNDEZ-VELA SALGADO, Edmundo. Diccionario de Política Internacional. Editorial Porrúa, S.A., 4ª edición, México, 1997.

MARTINEZ PICHARDO, José. Lineamientos para la Investigación Jurídica. Editorial Porrúa, S.A., México, 1994.

MEJAN, Luis Manuel. El Derecho a la Intimidad y a la Informática. Editorial Porrúa, S.A., México, 1994.

PADILLA SEGURA, José Antonio. Informática Jurídica.. Editorial SITESA-IPN, México, 1991.

PAVON VASCONCELOS, Francisco. Comentarios de Derecho Penal. Editorial Porrúa, S.A., 8ª edición, México, 1997.

PINA, Rafael De y Rafael De Pina Vara. Diccionario de Derecho. Editorial Porrúa, S.A., 21ª edición, México, 1995.

RENDÓN ORTIZ, Gilberto. Internet para Principiantes. Editorial Selector, México, 1996.

ROJAS AMANDI, Víctor Manual. El Uso de Internet en el Derecho. Editorial Oxford, México, 1991.

TELLEZ VALDEZ, Julio. Derecho Informático. Editorial Mc Graw Hill, 2ª edición, México, 1996.

_____. Derecho Informático. Col. El Derecho en México una visión de conjunto. UNAM, México, 1991.

LEGISLACIÓN.

CONSTITUCIÓN DE LOS ESTADOS UNIDOS MEXICANOS. Editorial SISTA, México, 2001.

LEY FEDERAL DEL DERECHO DE AUTOR. Editorial SISTA, México, 2001.

CÓDIGO PENAL FEDERAL. Editorial SISTA, México, 2001.

CÓDIGO PENAL PARA EL DISTRITO FEDERAL. Editorial SISTA, México, 2001.

CÓDIGO PENAL PARA EL ESTADO DE SINALOA. Editorial ANAYA, México, 1996.

CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL ESTADO DE SINALOA. Editorial ANAYA, México, 1996.

TRATADO DE LIBRE COMERCIO.

OTRAS FUENTES.

Revista "www. vivir en internet". Publicación mensual septiembre del 2001.

PAGINAS DE INTERNET CONSULTADAS.

www.aol.com.mx.

www.apuntes.lasalvación.com.

www.bufetalmeida.com.

www.cnnenespañol.com.

www.colosus.rhon.itam.mx/sriosma/.

www.ctv.es/users/mqp/delitos.htm.

www.derecho.unex.es/biblioteca/latderinformatico.htm.

www.df.gob.mx

www.download.com.

www.fundesco.es/seminarios/actas/los/gv.html.

www.gobernación.gob.mx

www.infojuridicas.unam.mx/cnsinfo/fed00.html.

www.informaticajuridica.com/trabajos/doc/virus_sinvacuna_doc.

www.iurislex.org/.

www.juridicas.unam.mx/legislac/.

www.microsoft.com.isapi.

www.monografias.com/indexshtml.

www.org.org.mx/judicatura/

www.scjn.gob.mx

www.terra.com.mx.

www.tiny.uasnet.mx/prof/cln/der/silvis/index.html.

www.t1msn.com.mx

www.unam.com.mx

www.yahoo.com.mx

CASO !HISPAHACK: LA SENTENCIA

JUZGADO DE LO PENAL NÚM. DOS BARCELONA

En Barcelona, a veintiocho de mayo de mil novecientos noventa y nueve.

El Ilmo. Sr. D JUAN CARLOS LLAVONA CALDERON, Magistrado-Juez del Juzgado de lo Penal nº 2 de los de esta capital, ha visto en juicio oral y publico las presentes actuaciones de Procedimiento Abreviado Nº 130/99-E de la Ley Orgánica 7/1988, de 28 de diciembre, dimanante de Diligencias Previas nº 1206/98 del Juzgado de Instrucción nº 20 de Barcelona, seguidas por un presunto delito de daños contra el acusado JFS en libertad provisional por esta causa, defendido por el Abogado Carlos A. Sánchez Almeida y representado por el Procurador Carlos Pons de Gironella, siendo parte acusadora el Ministerio Fiscal.

ANTECEDENTES DE HECHO

PRIMERO.- Por el Juzgado de Instrucción nº 20 de Barcelona se incoaron Diligencias Previas nº 1206/98, en virtud de atestado instruido por la Unidad de Policía Judicial de la Guardia Civil, habiendo formulado el Ministerio Fiscal escrito de acusación contra JFS, por lo que se acordó la apertura del juicio oral, correspondiendo su conocimiento a este Juzgado, que inició el Procedimiento Abreviado nº 130/99-E.

SEGUNDO.- El acto del juicio oral se ha celebrado el pasado 26 de mayo, practicándose en el mismo las pruebas siguientes: Interrogatorio del acusado, Testifical de JBT, BVV, los agentes de la Guardia Civil titulares de los carnets nº 26.001.263 y 118.189, AMT y MFB, respectivamente, Pericial a cargo de JIG y PFG, y Documental.

TERCERO.- El Ministerio Fiscal en sus conclusiones definitivas estimó los hechos como constitutivos de un delito de daños, previsto y penado en el Art. 264-2 del Código Penal, del que era autor el acusado, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, solicitando que se le impusiera la pena de dos años de prisión y multa de dieciocho meses a razón de 1000 pesetas de cuota diaria, con responsabilidad personal subsidiaria de 270 días y costas.

CUARTO.- La defensa del acusado, en su escrito de conclusiones provisionales elevadas a definitivas, manifestó su disconformidad con las conclusiones del Ministerio Fiscal, solicitando su libre absolución.

HECHOS PROBADOS

Así expresamente se declaran, que a las 4,16 horas del día 11 de septiembre de 1997 se produjo un acceso no autorizado a través de Internet en los ordenadores ubicados en las dependencias de la UPC, desde un ordenador situado en el campus de V., en G., de la Universidad de O. denominado "proy6.etsiig.uniovi.es", llegando a obtener los privilegios del administrador del sistema en al menos dieciséis máquinas servidoras e instalando programas "sniffers" destinados a capturar información que circula por la red del sistema, en concreto identificadores y claves de acceso de otros usuarios, enviando los datos obtenidos a través de Internet a un ordenador denominado "ftp.laredcafe.com" ubicado en el bar LRCC sito en la calle C. de P. de M., almacenándolos en el directorio denominado "jfs" correspondiente al usuario "Hispahack", sin que conste acreditado que el acusado JFS, mayor de edad y sin antecedentes penales, participase en esa entrada ilegal, obtención y transferencia de datos informáticos.

FUNDAMENTOS DE DERECHO

PRIMERO.- Al abordar con mayor detenimiento las cuestiones previas planteadas por la defensa del acusado al comienzo del juicio oral, enseguida se advierte la escasa consistencia de las alegaciones en que se funda la declaración de nulidad pretendida, pues si por una parte, y con referencia a las investigaciones realizadas por los miembros de la Guardia Civil adscritos a la Unidad Central Operativa, éstas no precisaban de denuncia previa por parte de los afectados, ya que, aunque así sea con relación a determinadas figuras delictivas que pueden cometerse por medios informáticos o telemáticos, como es el caso del descubrimiento y revelación de secretos que tipifica el Art. 197 del vigente Código Penal, y conforme establece el Art. 201.1 del mismo Código, no ocurre lo mismo, sin embargo, con relación a otros delitos como es precisamente, aquél en que se centra la acusación formulada en esta causa, tipificado en el Art. 264.2 del citado cuerpo legal, cuya persecución y castigo no se condiciona a la previa denuncia, siendo ésta en todo caso un requisito de procedibilidad una vez determinada la conducta punible y su calificación jurídico penal, pero no un óbice para la actuación de investigación de conductas supuestamente delictivas, al margen de su concreta calificación, que corresponde a las fuerzas y cuerpos de seguridad del Estado, por otra parte, y en lo que atañe a la pretendida vulneración del derecho fundamental a la intimidad y al secreto de las comunicaciones que corresponde al acusado, debe

señalarse que las investigaciones realizadas respecto del mismo no han incidido en ninguno de esos derechos, y su identificación fue posible, según explica el atestado, después de haber recibido un mensaje de correo electrónico alertando sobre las actividades de unos supuestos "hackers" informáticos, al que se adjuntaban fotografías de varios de los integrantes de ese grupo, uno de ellos identificado con las iniciales Jfs, accediendo posteriormente a una página de información pública ubicada en un proveedor de Internet de Estados Unidos que, según la información contenida en la misma, pretendía ser la página de un grupo llamado "Hispahack", y en la que aparecía un artículo atribuido a jfs, y tras realizar diversas gestiones lograron localizar en Internet un ordenador conectado de nombre "jfs.hispahck.org" ubicado en la empresa GL de Gibraltar que, por medio de AAO, lograron averiguar que había sido dado de alta en la red por el acusado. Bien es cierto que para la identificación de otros supuestos integrantes de aquel grupo se acudió al proveedor en España de Internet a fin de conocer su identidad mediante su dirección de correo electrónico, pero además de no ser éste el caso del aquí acusado, tampoco cabe entender que ello constituyese vulneración alguna del derecho fundamental al secreto de las comunicaciones, ya que no se tuvo acceso al contenido de ningún mensaje transmitido mediante correo electrónico y sí sólo al nombre de la persona que utilizaba la dirección correspondiente, de la misma manera que podría haberse identificado a un abonado del servicio telefónico a través de su número de abonado, no suponiendo ello violación de derecho fundamental alguno, ni siquiera de las prescripciones que para el acceso y transmisión de datos personales contiene la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal, pues la propia Ley excluye de la necesidad del consentimiento del afectado la recopilación de datos que requiera el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (Art. 6.2), especialmente cuando la información al afectado impida o dificulte la persecución de infracciones penales o administrativas (Art. 22.1), quedando en todo caso limitada la recogida y tratamiento automatizado de datos de carácter personal por las fuerzas y cuerpos de seguridad del Estado, sin el consentimiento de las personas afectadas, a aquellos supuestos y categorías de datos que resulten necesarios para la represión de infracciones penales (Art. 20.2). En suma, no cabe sino reiterar aquí nuevamente el rechazo a la pretensión de nulidad de parte de las actuaciones llevadas a cabo en esta causa que plantea la defensa del acusado. Por lo demás, y en contra de lo que sostiene dicha parte, no se cuestiona aquí el ejercicio de la libertad de expresión través de Internet, sino que el enjuiciamiento se centra en una actividad que con la expresión anglosajona "hacking" (intrusismo informático) hace referencia a un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado, conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables, y aún merecedoras de

sanción penal si -como suele ser lo habitual- atentan contra sistemas o equipos informáticos particularmente relevantes que, por razón del contenido de la información que procesan o almacenan y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales, afectan gravemente a un interés supraindividual o colectivo, de manera que plantear en esta sede una adecuada tutela penal autónoma frente al intrusismo informático no puede en modo alguno considerarse un exceso de reacción penal.

SEGUNDO.- Los hechos que se declaran probados en esta resolución son el resultado de una apreciación en conciencia de las pruebas practicadas en el juicio, conforme a lo dispuesto por el Art. 741 de la Ley de Enjuiciamiento Criminal, y así, en efecto, el informe elaborado en su momento, y ratificado en dicho acto plenario como testigo, por JBT refiere la existencia de un ataque a los sistemas informáticos de la UPC con resultado de obtención de privilegios de administrador e instalación de programas "sniffers", afectando al menos a dieciséis máquinas servidoras y haciendo uso de herramientas para capturar información en las menos cinco de ellas, concretamente identificadores y claves de acceso de otros usuarios, ataque realizado desde una máquina perteneciente a la UO y que remitió la información obtenida a otra máquina instalada en PM (folios 15 y 16). No cabe reputar acreditada, sin embargo, la autoría que de tales hechos se atribuye al acusado JFS, pues si bien existen fundadas sospechas de que pudo tener algún tipo de participación en ellos, ya que por una parte él mismo reconoce su pertenencia al grupo denominado "Hispahack" y la utilización del apodo "jfs" , que corresponden al usuario y directorio, respectivamente, del ordenador instalado en el bar "LRCC" al que se transfirieron los datos obtenidos en el sistema informático de la UPC, habiéndose comprobado además, en el examen del disco duro de los ordenadores que tenía en su domicilio de Martorell, intervenidos en la diligencia de entrada y registro practicada en el mismo, según expresa el perito JIG, la presencia de programas para aprovechar las vulnerabilidades de otros sistemas, ficheros de claves cifradas de usuarios de servidores y resultados de 'sniffers" que incluyen identificadores de usuarios y llaves de acceso a máquinas de la UB y a la UO, sin embargo tales sospechas no alcanzan la categoría de indicios bastantes como para desvirtuar totalmente la presunción de inocencia en cuanto a la concreta participación que en esos hechos se le atribuye, pues si por una parte el acceso al ordenador de PM, y a través de él al directorio "jfs", se hallaba al alcance de cualquiera que lo hiciese a través de usuario "Hispahack", en el que el mismo perito, al examinar el disco de dicho ordenador también intervenido tras la diligencia de entrada y registro practicada en el local donde se hallaba instalado, ha comprobado la existencia de ficheros de datos y utilidades relacionadas con los problemas de seguridad de los sistemas Unix, conteniendo información sobre vulnerabilidades de máquinas, programas para explotar fallos de seguridad, "sniffers" y otras utilidades conocidas como "utilidades de hacking", al alcance de cualquiera que pudiera

acceder a dicho ordenador como usuario "Hispahack", ni el informe de FOF sobre el ordenador de la Universidad de Oviedo, a través del cual se accedió a los sistemas de la UPC, ha podido definir el origen de la intrusión no permitida a través de Internet, constatando la existencia de un directorio compartido accesible a cualquier máquina, sin claves, montado por otras dos máquinas desconocidas, ni el examen de los ficheros contenidos en los discos instalados en los ordenadores del acusado ha permitido establecer que éste poseyese información de aquellos sistemas. Ya el propio testigo JBT admite que posiblemente la persona que usaba los "sniffers" era la misma persona que los instaló, pero no puede afirmarlo con certeza, el perito JIG afirma que los ficheros con códigos de usuarios y llaves de paso detectados en las máquinas del acusado fueron generados por "sniffers" que alguien (sin precisar quién) instaló en servidores de diferentes organizaciones, y conviene con el también perito PFG en que entre tales ficheros no se hallaba ninguno de password de la UPC. No apareciendo acreditado, por tanto, más allá de toda duda razonable, que fuese el acusado quien alteró los programas contenidos en el sistema informático de dicha Universidad haciendo necesaria su total reinstalación, que es la conducta sancionada penalmente que se le atribuye, no cabe llegar a otro pronunciamiento que el de su libre absolución.

TERCERO.- Procede declarar de oficio las costas ocasionadas de conformidad con lo establecido por los Art. 239 y 240.1º de la Ley de Enjuiciamiento Criminal.

Vistos los preceptos legales citados y demás de general y pertinente aplicación;

FALLO

Que debo de absolver y absuelvo libremente a JFS del delito de daños de que venía siendo acusado en este procedimiento, declarando de oficio las costas ocasionadas.

Líbrese y únase certificación de esta resolución a las actuaciones, con inclusión de la original en el Libro de Sentencias.

Así por esta mi sentencia, definitivamente juzgandó, lo pronunció mandó y firmó.