

Voces: INFORMATICA ~ RESPONSABILIDAD PENAL ~ SOFTWARE

Título: Virus informáticos y responsabilidad penal

Autor: Palazzi, Pablo A.

Publicado en: LA LEY1992-E, 1122

SUMARIO: I. Introducción. -- II. Virus informáticos. -- III. Casos en el derecho extranjero. -- IV. La posible solución en nuestro derecho penal: artículos 183 y 184 del Código Penal. -- V. Conclusión.

I. Introducción

Es innegable la rapidez con que la informática se ha introducido en el mundo actual. El avance de las nuevas tecnologías a pasos agigantados, la difusión de sus ventajas, la estandarización de los sistemas y la disminución de los costos --entre otros motivos-- han posibilitado el acceso de gran cantidad de personas a una computadora.

Por informática entendemos "los aspectos de la ciencia y tecnología específicamente aplicables al tratamiento de la información y, en particular, al tratamiento automático de datos"⁽¹⁾.

La informática no es un fin en sí mismo sino un medio para realizar determinados objetivos. Esta utilidad es, por otra parte, amplísima, lo que expande su campo de aplicación.

Pero no todo uso que se le dé a la informática puede llegar a ser bueno: es necesario emplearla correctamente, es decir, orientada al fin para el que sirve y respaldándola siempre con valoraciones éticas. Lo contrario implicaría no sólo desvirtuarla sino malograr los objetivos que ella se propone ayudar a alcanzar.

No hace mucho tiempo atrás se descubrió una organización de personas que traficaba datos informáticos. El hecho ocurrió en España y lo que dieron cuenta las informaciones periodísticas era la falta de leyes que regularan estas conductas disvaliosas ⁽²⁾.

Desde hace varios años, también otra situación altera el adecuado funcionamiento de la informática, atacando la salud de un sistema y se trata del fenómeno conocido como "virus".

Estos programas de computación de carácter dañino, que surgieron en principio como un juego al que se dedicaban programadores expertos en sus horas de ocio, amenazan con ser hoy una nueva epidemia, no biológica, como las que se padecían en la Edad Media y lamentablemente todavía padecemos hoy, sino de carácter tecnológico. Ya en junio de 1991 la revista International Business Week anunciaba la existencia de más de 500 virus distintos y daba a conocer una encuesta en la que el 26 % de las 200 compañías entrevistadas admitían haber sido atacadas por algún tipo de virus ⁽³⁾.

Hoy la cantidad de virus informáticos existentes llega al millar.

Recientemente, los medios periodísticos de nuestro país y del mundo, crearon una alarma general por la activación del virus "Michelangelo". Los consejos dados por los especialistas evitaron que se perdiera la información almacenada en las computadoras. De haber ocurrido lo contrario, los perjuicios patrimoniales habrían sido enormes.

II. Virus informáticos

1. Concepto

Un virus es un programa de ordenador, generalmente anónimo, que lleva a cabo acciones que resultan nocivas para el sistema informático y cuyo funcionamiento queda definido por las propiedades siguientes: hacer copias de sí mismo, de forma homogénea y en partes discretas, en un fichero, disco u ordenador distinto al que ocupa ⁽⁴⁾.

El profesor L. J. Kuttan define un virus informático como un programa de computación que puede diseminarse de una computadora a otra sin la intervención de un usuario y sin que éste tenga conciencia de la transmisión. A su vez cada programa infectado puede infectar a otro. Una vez allí toma el control de la computadora ⁽⁵⁾.

Carlos M. Correa, en su libro "Derecho informático" habla de "programas virus" como "instrucciones que se infiltran automáticamente en otros programas y archivos"⁽⁶⁾.

Para nosotros un virus de computación es un conjunto de instrucciones (programa), invisibles al usuario, que tienen la facultad de hacer copias de sí mismas y de producir un efecto que fue determinado con anticipación por su autor.

2. Clasificación

Una clasificación rigurosa y técnica escaparía al marco de este trabajo. Por tanto nos limitaremos a dar sólo aquellas que sean de interés para una primera aproximación al tema.

Ya hemos hablado de lo que es un virus y hemos esbozado varias definiciones. Existen también otra clase de programas infecciosos: los llamados "bomba de tiempo" y el "caballo de troya", que se diferencian del virus por carecer de la facultad de autorreplica.

La "bomba de tiempo" o "bomba lógica" (logic bomb) es un programa de apariencia benigna, pero que activa sus efectos nocivos ya sea por el paso del tiempo (se activan si arriba a determinada fecha) o porque el usuario realiza una serie de operaciones que son habituales pero que el programa identifica como la señal para empezar a actuar.

El "caballo de troya" (trojan horse) es también un programa de apariencia normal, pero que una vez ejecutado destruye la información almacenada en la computadora.

Otro factor de clasificación usado es la peligrosidad del virus. Así se habla de virus de primera y segunda generación.

En un principio, éstos eran de una estructura relativamente sencilla, fácilmente detectables por sus efectos. Actualmente, los virus de primera generación han dejado su lugar a los de segunda. Estos últimos fueron desarrollados, merced a depuradas técnicas de programación, teniendo en cuenta la existencia de sistemas antivirus y de seguridad, con posibilidad de autoencriptarse para dificultar su detección; tienen un código más corto y efectivo y actualmente son los más peligrosos. Son hasta capaces de contaminar una red y "darse cuenta" de que están siendo revisados y eliminados por un antivirus.

Si bien éstas son clasificaciones según el modo de trabajo o peligrosidad del virus, es posible afirmar que cada virus da a su vez lugar a una nueva clase por las distintas características que lo diferencia de los demás. Hay que agregar que de cada virus se hacen mutaciones locales, de lo que emergen las "variedades" de virus. En nuestro país existen variedades del virus proveniente de Jerusalén (llamado "Jerusalém-Mendoza" por los expertos locales) e incluso virus totalmente creados en Argentina.

Los virus también se pueden clasificar, en cuanto a sus efectos, en nocivos o inofensivos. El único daño que producen los inofensivos es un retraso en el funcionamiento del ordenador. Actualmente, la mayoría de los virus son de carácter dañino.

3. Funcionamiento

Un virus funciona de acuerdo al siguiente mecanismo: luego de ser programado por el autor, el virus es insertado en un lugar al que tengan acceso muchas personas (una computadora de uso común, una red pública, una base de datos). Allí el programa irá sucesivamente infectando --mediante el proceso de hacer copias de sí mismo-- todos los diskettes que sean introducidos en esa computadora. Estos diskettes serán llevados a otro ordenador, que se infectará y el ciclo comenzará nuevamente, hasta que el virus sea detectado y eliminado o produzca sus efectos. Generalmente --y como ya lo hemos expresado-- los efectos de los virus son destructivos. El daño se puede producir sobre los diskettes (7) o sobre el disco rígido (8).

También puede afectar a la memoria de la computadora.

La estandarización de los sistemas fue uno de los factores que contribuyeron a la aparición y propagación del virus informático. Si las computadoras no operaran de la misma manera los virus no podrían pasarse de unas a otras.

El motivo por el cual se hace este tipo anómalo de programas todavía no es muy claro. En un momento se pensó que los propios fabricantes de software crearon los virus para evitar la "piratería". Luego se esbozó la teoría de que los mismos vendedores de antivirus estaban relacionados con estos programas. Otra tesis sostiene que se trata de hábiles programadores que buscan demostrar sus conocimientos.

III. Casos en el derecho extranjero

El adelanto que Estados Unidos representa en materia de alta tecnología corre a la par de sus leyes. En 1984 se sancionó la "Ley contra el abuso y fraude informático" (Counterfeit acces device and computer fraud and abuse), modificada luego en 1986.

Esta ley tipifica penalmente el acceso no autorizado a sistemas informáticos operados por el gobierno y en particular a los asociados a la defensa nacional, las relaciones externas, la energía atómica, y a los de instituciones financieras (9).

La mayoría de los Estados ha ido adaptando sus leyes penales al incluir figuras que contemplan los distintos delitos informáticos a los que ha dado lugar la constante evolución de la técnica en esta materia (10).

Uno de los precursores ha sido el Estado de California. A finales de 1988 modificó su Código Penal, haciendo constar que todo aquel que "conscientemente acceda y, sin permiso, añada, altere, erosione, borre o destruya datos, software o programas de ordenador, sistema informático o red de ordenadores..." es culpable de ofensa pública. La pena que se establece para este delito de ofensa pública es de una multa de 10.000 dólares, la confiscación del equipo informático del acusado y prisión hasta un período máximo de tres años (11).

También el Estado de Minnesota sancionó una ley que prohíbe la distribución intencional de programas computacionales destructivos, que se definen como cualquier software que degrade el rendimiento e inhabilite el computador, periféricos o sus sistemas. Además, cualquier programa que produzca datos no autorizados (lo que incluye información que sólo ocupa espacio) o altera la información también es considerado destructivo. La ley fija penas que se gradúan desde una pequeña multa y 90 días de prisión, por delitos que no ocasionen daño

al computador, hasta 10 años en prisión y 50.000 dólares de multa por delitos que provoquen más de 2.500 dólares de daño.

Maryland y West Virginia son otros Estados que se sumaron en 1989 a los que poseen leyes sobre virus computacionales (12).

En el caso del Estado de Virginia, el Código Criminal considera "propiedad" el "tiempo de computador o de servicios de procesamiento de datos" y por tanto incrimina el uso no autorizado de ellos (13).

Aunque se registraron varios casos judiciales de virus en los Estados Unidos, el primero que adquirió resonancia pública, a nivel tanto nacional como internacional fue "United States vs. Morris".

En noviembre de 1988, Robert Tappan Morris, estudiante de informática en la Universidad de Cornell e hijo de uno de los más prestigiosos expertos en seguridad de sistemas informáticos del gobierno introdujo un virus en la red ARPANET. Esta red de computadoras posee miles de terminales en varios continentes y fue fundada para tratar material no clasificado entre universidades e institutos de investigación públicos y privados de los Estados Unidos y otros países. El virus fue contaminando toda la red hasta saturarla en pocas horas. Esto provocó el bloqueo de las líneas de computación y de las memorias de las computadoras de la red. Más de 6000 ordenadores quedaron afectados. Entre ellos algunos del Pentágono, la NASA, el Mando Aéreo Estratégico, la Agencia Nacional de Seguridad (NSA), el Ministerio de Defensa, los laboratorios Lawrence Livermore de Berkeley (California) y las Universidades de Princeton, Yale, Columbia, Harvard, Illinois, Purdue, Wisconsin y el Instituto de Tecnología de Massachussets. Incluso se llegó a afectar ordenadores de la República Federal de Alemania y Australia que estaban también conectados a la red.

Morris fue detenido y el juicio comenzó en enero de 1990, en el tribunal del distrito de Siracusa, Nueva York. La Fiscalía solicitó una pena de prisión de cinco años y una multa de 250.000 dólares. La opinión pública nacional estaba dividida: por una parte se veía a Morris como a un terrorista informático, pero otro sector lo consideraba un genio que sólo buscó demostrar sus habilidades y lo exponían como baluarte de uno de los pocos campos en el que Estados Unidos todavía mantiene su liderazgo: la producción de software. Finalmente Morris fue condenado solamente y merced a una excelente defensa, a tres años de libertad condicional, 10.000 dólares de multa y 400 horas de trabajo comunitario (community service).

Esta pena en los Estados Unidos fue posible aplicarla porque existe una ley específica sobre el tema, pero son pocos los países que se encuentran en tal situación.

En España, que no tiene normas especiales para prevenir o sancionar delitos informáticos se han registrado casos judiciales, siendo dignos de mención dos de ellos que resumimos seguidamente.

Un programador de una empresa que se dedicaba a producir software para los ayuntamientos españoles, envió un diskette con supuestas instrucciones para corregir defectos en el programa comercializado. Al poco tiempo esos clientes advirtieron que existía un virus en sus ordenadores provenientes de ese programa. El inescrupuloso personaje inmediatamente dejó de trabajar para la empresa y junto a otro empleado de la misma creó una nueva sociedad para ofrecer los servicios del caso a los clientes damnificados.

Pero, ambos autores fueron descubiertos y denunciados por la empresa y la Asociación de Empresas Españolas Fabricantes de Software, ante el Juzgado N° 8 de Barcelona en el mes de mayo de 1989 (14).

Esta clase de procesos tramitan en España bajo aplicación de las leyes penales comunes(15).

La ley sueca de 1983 reprime el mero acceso a un sistema de procesamiento de datos (16).

Por su parte, un proyecto de ley informática del Ministerio de Justicia de Chile (abril de 1986) prevé que "cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras, un soporte lógico o programa de la computadora o, los datos contenidos en la misma, en la base, sistema o red"(17).

IV. La posible solución en nuestro derecho penal: artículos 183 y 184 del Código Penal

Tanto en el ámbito penal como en el civil, en la Argentina no existe un cuerpo orgánico de disposiciones que regule en forma específica los delitos informáticos.

Actualmente, uno de los graves problemas que enfrenta la justicia penal es el de si es punible o no lo es copiar sin autorización, programas de computación. La dificultad primigenia se basa en si la ley 11.723 del año 1933 (Adla, 1920-1940, 443), de propiedad intelectual está contemplado el software como obra intelectual protegida (18).

En el fuero penal no existen todavía sentencias definitivas al respecto.

Sin embargo, cabe acotar que existe jurisprudencia civil que niega al software la protección jurídica bajo el derecho de autor (ley 11.723).

O sea, que sobre el tema hay incertidumbre, lo que lógicamente conspira contra la seguridad jurídica de las personas.

Sin perjuicio de ello, analizaremos la situación de una persona que introduce un virus de efecto dañino en un ordenador, a la luz de nuestra actual ley penal (19).

La mayoría de los delitos contra la propiedad requiere para su consumación la transferencia ilícita de un bien a otro patrimonio aunque no fuera el del culpable y aunque no siempre fuere esencial ese elemento de transferencia y bastará, en muchos casos, el solo despojo o la privación del bien.

Pero existe una manera típica de causar perjuicio, un puro perjuicio en la propiedad --dice Soler--, y que conduce a la pérdida misma de la cosa, a la anulación del derecho real, y consiste en la destrucción de la cosa misma sobre la cual el derecho era ejercido (art. 2604, Cód. Civil) (20). Se trata del delito de daño.

El título VI del Código Penal referido a los delitos contra la propiedad, incluye una figura básica de daño (art. 183) y una figura agravada (art. 184).

El art. 183 del Cód. Penal fija el delito de daño en los siguientes términos: "Será reprimido con prisión de un mes a dos años, el que destruyere, inutilizare o hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

El objeto material del daño está constituido por una cosa mueble o inmueble o un animal total o parcialmente ajeno.

El virus informático produce un daño borrando la información contenida en la computadora. Es importante aclarar que no es la computadora en sí misma el objeto dañado, sino la información que ésta posee.

Ahora bien ¿Puede la información almacenada en el disco rígido, el diskette o la memoria de una computadora ser objeto del delito de daño?

La información que se encuentra en una computadora adopta la forma de energía, que podrá ser eléctrica o magnética según el soporte que la posea. La cuestión reside en determinar si la energía puede ser considerada una cosa. El art. 2311 del Cód. Civil, reformado por la ley 17.711 ha otorgado carácter de cosa a la energía (21).

Pero la ley no dice que las energías (electricidad, energía atómica o atracción magnética) son cosas, sino que a aquéllas se les aplicará las mismas disposiciones que a las cosas, por lo que en definitiva les reconoce la calidad de tales. En derecho lo que cuenta son los efectos --sostiene Borda--; luego, si las energías apropiables tienen igual condición que las cosas, son cosas (22).

La opinión de otorgar carácter de cosa a la energía era predominante tanto en la jurisprudencia como en la doctrina antes de la reforma de 1968 del Código Civil (23).

La Cámara del Crimen de la Capital ha sostenido que "...al estar legislada la energía como cosa, el hurto se consume con las diversas utilidades del fluido (eléctrico) ..." (24). Incluso, la jurisprudencia ha aceptado que la señal emitida por una empresa que transmite imágenes de televisión implica una energía que como tal es susceptible de tener valor (art. 2312, Cód. Civil) por lo que su apoderamiento mediante una conexión clandestina configura el delito de hurto (25).

La energía magnética que está en la superficie de un disco rígido o un diskette, por ser apropiable, se rige, entonces por las disposiciones de las cosas. Igual criterio se aplicará a la energía eléctrica que se encuentra en la memoria de un ordenador. Ambas pueden ser alteradas por un virus. Entonces, la información contenida en una computadora (ya sea en un diskette, en el disco rígido o en la memoria) llega a poseer la entidad suficiente para ser reputada cosa a los efectos de aplicarles las mismas disposiciones. Por otro lado la doctrina moderna le atribuye a la información un valor en sí misma como mercancía, y la posibilidad de un derecho de propiedad sobre ella (26).

La acción consumativa en el delito de daño --refiere Soler-- es designada con la frase "destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare". Agrega que una cosa ha sido destruida cuando por efecto de la acción no existe más en la sustancia y forma que la especificaban y le daban valor (27).

La jurisprudencia sostiene que el delito de daño no exige que la cosa mueble o inmueble quede totalmente destruida o inutilizada, bastando para su consumación que la restitución del bien a su estado anterior demande algún gasto, esfuerzo o trabajo (28). En computación, es posible muchas veces recuperar los datos que se han borrado, incluso generalmente la regla es tener un back-up (copia de respaldo) de la información que se posee, para que en caso de pérdida de ésta, el daño sea mínimo. Creemos que, ello no obsta a que el delito se encuentre consumado en esta situación.

Núñez dice que la destrucción, la inutilización, el daño o la desaparición de la cosa se pueden cometer con cualquier medio y en cualquier modo, siempre que no califiquen el delito o no lo conduzcan a otro más severamente penado (29). Al incluir el tipo penal del art. 183 la frase "cualquier modo" afirmamos que el accionar de un virus informático encuadra en la figura básica del delito de daño.

Refiriéndose al elemento subjetivo de este delito, Núñez dice que para que un daño en la cosa ajena sea punible en los términos del art. 183 del Cód. Penal, se requiere un *damnum injuria datum*, esto es, un daño injuriosamente producido, por haber sido causado por el autor a sabiendas de su injusticia y de propósito (30).

Es decir que la característica subjetiva del delito de daño reside en que el menoscabo de la propiedad ajena es un fin en sí mismo (31). El caso de una persona que libera un virus al dominio público, sabiendo que en determinada fecha o bajo determinadas condiciones destruirá la información del ordenador donde se encuentre, reúne los elementos requeridos para el dolo de esta figura. Incluso se podría llegar a decir que el virus afecta bienes indeterminados y podría entrar dentro de las disposiciones que protegen la seguridad común, como veremos más adelante.

El sujeto activo puede ser tanto el autor del virus (el programador), como el que infecta un ordenador (caso del empleado despedido que desea vengarse) o el que facilitó su propagación pudiendo evitarlo.

El art. 184 presenta una figura agravada según se den ciertas situaciones. Es de especial interés para el tema que estamos tratando el inc. 5°. Este inciso proviene del inc. 5° del art. 220 del Cód. Penal reformado de 1886 lo mismo que el proyecto de Código Penal de 1881, se refería a archivos, registros, bibliotecas o museos públicos. Núñez nos expresa que archivos son las colecciones ordenadas, públicas o privadas, de documentos o papeles de importancia o interés (32).

Seguidamente dice Núñez que los registros son los asientos, por regla públicos, de actas o antecedentes sobre determinados asuntos o materias. Por último define bibliotecas como conjuntos o colecciones considerables de libros, revistas, periódicos o folletos existentes en un determinado lugar para el uso público o particular (33).

Conforme estas definiciones un archivo o registro electrónico quedaría comprendido dentro de ellas, ya que no hacen diferencias al soporte en el cual se encuentre. Por último, una biblioteca es asimilable a un banco de datos informatizado, dada la extensión que ambos poseen. Se diferencian --nuevamente-- en el medio de almacenamiento de la información. No hay diferencia entre un soporte magnético y uno de papel.

Por ser un delito material, requiere un efectivo daño. Por lo tanto no basta solamente que el sujeto activo contamine una computadora, sino que será necesario para la consumación que el programa virósico produzca sus efectos perjudiciales. Pero, el delito puede quedar en grado de tentativa si se dan las circunstancias del art. 42 del Cód. Penal. Esto incluye un error de programación que haga que el virus no funcione correctamente, un programa antivirus que lo detecte y lo elimine o la inactividad de la computadora el día en que el programa dañino se activara.

Dada la importancia del contenido de los elementos almacenados en medios informáticos, creemos que es necesario considerar ciertos casos como figuras agravadas del delito de daño.

La posibilidad de cometer estos delitos a gran distancia, y con una diferencia considerable de tiempo entre el momento en que se realiza la acción y el momento en que se consuma, plantea un complicado problema de carácter probatorio. Contribuye a ello la circunstancia de que el virus, al destruir la información almacenada en el ordenador se destruye también a sí mismo (y esto ocurre con más frecuencia en las últimas generaciones de virus) sin dejar ningún rastro. De esta manera, no es posible comprobar si el borrado de la información se debió realmente a un virus o a un error interno de la computadora (bajas o picos de tensión, falla en el booteo(34) o encendido del ordenador o defectos en el disco rígido, como ser una falla en el hardware del equipo, etc). Estos hechos harían muy difícil atribuir a la autoría de un "virus" la destrucción de la información. En estas circunstancias sería imposible saber quién fue el autor del virus. Como expresa Fred Cohen "...a diferencia de otras conductas disvaliosas (asalto a bancos, pongamos por caso, u homicidio), el diseminar un virus en una computadora es un acto sutil que no deja rastro visible inmediatamente..."(35).

Es regla general que los delitos informáticos son descubiertos por la confesión de quien los hizo (caso "Morris", por ejemplo) o por la denuncia del individualmente perjudicado. Generalmente las empresas afectadas prefieren no dar a conocer estas fallas de sus sistemas de seguridad.

Si bien en nuestro país la informática no llega a ser de una extensión tan importante como en otras naciones, creemos que la afectación a los sistemas informáticos por parte de un virus no sólo puede quedar individualizado como un delito contra la propiedad. Es posible prever que en un futuro mediato las computadoras sean tan comunes, que gran parte de las conductas que se realizan cotidianamente sean coordinadas por éstas. Un virus que las afecte, no sólo estaría atacando el bien jurídico de la propiedad (Título VI, Código Penal), sino incluso podría vulnerar tipos de delitos contra la seguridad pública (Título VII, Código Penal), poniendo en peligro bienes indeterminados. Como dice Soler, en estos casos el bien jurídico final está defendido por una doble coraza, ya que se prohíben determinadas acciones no sólo en cuanto importan la violación o destrucción de ciertos bienes jurídicos, sino el peligro de que éstos se pierdan (36). Lo que se protege en esta clase de figuras es la seguridad. Y el correlativo de la idea de seguridad es la idea de peligro, no ya de lesión (ver por ejemplo la ley sueca citada ut supra). Pensamos que el casuismo actual de las figuras del título nombrado no permite encuadrar esta clase de hechos en alguna de sus normas. Por ejemplo, si un virus altera la información de la computadora que contiene los legajos de los pacientes de un hospital, los tratamientos que en

consecuencia se apliquen podrían causar graves daños a la salud.

También podrían alterar las redes internacionales de información de la banca, las comunicaciones, los transportes y aun la defensa. Se crean situaciones de peligro general e indeterminado. A este tipo de infracciones se las llama delitos de peligro común.

V. Conclusión

Los nuevos medios tecnológicos que disponemos en la actualidad, usados disvaliosamente, crean serios obstáculos en el deseo de alcanzar la paz social.

Es así como la violación de la intimidad a través del acceso ilegítimo a bancos de datos informatizados, los fraudes cometidos por medio de computadoras, la reproducción ilícita de software, el espionaje industrial y la introducción de virus dañinos en sistemas informáticos, entre otros, se irán transformando en los nuevos delitos que deberá enfrentar la sociedad y que el derecho y especialmente las ciencias criminológicas deben resolver lo antes posible.

Estos "delitos informáticos" se caracterizan generalmente por:

a) su atipicidad: el delito es legislado a medida que se dan nuevos casos, pues en el ámbito penal el principio *nullum crimen, nulla poena sine praevia lege* (art. 18, Constitución Nacional) impide la aplicación de sanciones a hechos no previstos con anterioridad;

b) la falta de denuncias: las compañías afectadas prefieren guardar silencio, antes que dar a conocer sus fallas de seguridad y por el temor que sus clientes pierdan la confianza que han depositado en la empresa;

c) su dificultad probatoria: relacionado con el punto anterior por la falta de cooperación de los damnificados, y por lo expresado en los dos puntos siguientes;

d) extraterritorialidad: el virus puede ser programado en cualquier lugar del planeta y puede producir sus efectos en cualquier otra parte. El caso del virus "Brain" es más que elocuente: fue desarrollado en Paquistán por dos jóvenes programadores y descubierto en un periódico de Rhode Island, USA. Esto también plantea el problema de la ley a aplicar;

e) intemporalidad: la posibilidad de programar su ejecución en una determinada fecha. Ejemplos: el "Columbus Day Virus" que se activaba el 13 de octubre, el "Michelangelo" que se activa el 6 de marzo, el "Virus Argentina" que se activa en nuestras fechas patrias, el "Jerusalem Virus" que se activa todos los viernes 13, etcétera.

Estas dos últimas características fueron las que usó el profesor André Bertrand, cuando en el discurso de inauguración del 1er Congreso de Informática y Criminalidad celebrado en Buenos Aires definió los elementos de los delitos informáticos (37).

Como el lector habrá podido apreciar, nuevas realidades se presentan frente al mundo jurídico y le plantean un desafío. Aceptarlo es una tarea que se deberá afrontar tarde o temprano.

Estos hechos sobre los que hemos escrito presentan aspectos de nivel internacional. Creemos por ello que no sólo será suficiente una legislación a nivel nacional. Se requiere --para ser combatidos con eficacia-- la cooperación de organismos internacionales y de las propias Naciones entre sí. Consideramos que sería importante el intercambio de información y la elaboración de estrategias conjuntas que permitan luchar contra estos flagelos --que por sus características ya expresadas-- no sólo afectan a un país sino al mundo entero.

Así, el uso de convenciones internacionales (v.gr. la recientemente aprobada Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, ley 24.072 B. O. del 14/4/92 --Adla, LII-B, 1557--) que teniendo en cuenta fenómenos que superan las fronteras nacionales, buscan establecer pautas o normas--tipo para que los países puedan legislar en base a ellas (algo similar a las directivas de la CEE). No propendemos con ello a la existencia de un derecho penal internacional(38), sino a directivas de máxima y de mínima para encausar a los Estados en la regulación de estos problemas que generan las nuevas tecnologías.

El proceso de adaptación jurídica a los cambios sociales, económicos y tecnológicos es una tarea legislativa que deberá desarrollarse paulatinamente y en la medida que sea necesario, aprovechando la experiencia de las leyes, la jurisprudencia y la doctrina extranjeras.

Especial para La Ley. Derechos reservados (ley 11.723).

(1)ALTMARK, Daniel R., "Informática y derecho" N° 1, p. 6, Ed. Depalma, Buenos Aires, 1987.

(2)ver La Nación, del 11 y 12/1/92.

(3)"Have computers viruses turned into a plague?" en International Business Week, June 10, 1991.

(4)MUR, Alfonso, NIETO, Pablo y MOLINA, Jesús, "Virus informáticos", p. 15, Ed. Anaya, Madrid, 1989.

(5)L. J. Kutten es director de "Software Law Bulletin", una publicación norteamericana especializada en derecho informático. La definición fue dada en el Primer Congreso de Informática y Criminalidad celebrado en

Buenos Aires el 25 y 26 de noviembre de 1991.

(6)CORREA, Carlos M., "Derecho informático", p. 296, Ed. Depalma, 1987.

(7)El diskette o floppy disk es un disco de mediana capacidad que se usa para almacenar datos o transferir programas entre una computadora y otra. Posee una capacidad aproximada de 360 a 1000 Kbytes (entre 300.000 y 1.000.000 caracteres).

(8)El hard disk, disco duro o disco rígido es un disco de gran capacidad y velocidad que hoy en día posee cualquier ordenador personal. Estos discos se encuentran generalmente montados dentro de la unidad central. Poseen una capacidad aproximada de 40 a 120 Megabytes.

(9)CORREA, Carlos M., "Derecho informático", p. 298, Ed. Depalma, 1987.

(10)MUR, Alfonso, NIETO, Pablo y MOLINA, Jesús, "Virus informáticos", p. 69, Ed. Anaya, Madrid, 1989.

(11)Computación Personal, N° 66, octubre 1989, Santiago, Chile.

(12)MUR, Alfonso, NIETO, Pablo y MOLINA, Jesús, "Virus informáticos", p. 74, Ed. Anaya, Madrid, 1989.

(13)CORREA, Carlos M., "Derecho informático", p. 298, Ed. Depalma, 1987.

(14)MUR, Alfonso, NIETO, Pablo y MOLINA, Jesús, "Virus informáticos", p. 73, Ed. Anaya, Madrid, 1989.

(15)El Código Penal español prevé el delito de daño en los arts. 557 al 563.

(16)CORREA, Carlos M., "Derecho informático", p. 298, Ed. Depalma, 1987.

(17)CORREA, Carlos M., "Derecho informático", p. 298, Ed. Depalma, 1987.

(18)Los fallos civiles y penales pueden ser consultados en DAT (Revista del Derecho de la Alta Tecnología). Una interesante crítica al tema se puede ver en DOZO MORENO, Abel V., "La copia del programa de computación y el delito penal", Ed. Licurgo, Buenos Aires, 1991.

(19)La problemática civil fue analizada por DALL'AGLIO, Edgardo J. en su trabajo "La responsabilidad derivada de la introducción y propagación del virus de las computadoras" publicado en ED, 135-903.

(20)SOLER "Derecho penal argentino", t. III, p. 465.

(21)El art. 2311 del Cód. Civil dice: "Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación".

(22)BORDA, Guillermo, "Tratado de Derecho Civil, Parte General", t. II, p. 32, Ed. Abeledo-Perrot, Buenos Aires, 1980.

(23)De acuerdo: CApel. Rosario 12/6/56, JA, 1956-IV, 444; S. Buenos Aires, 7/7/53, LA LEY, t. 71, 447; CFed La Plata, 1/10/62, LA LEY, t. 110-913; SPOTA, t. 1, vol. 3, N° 1362 ter; SOLER, S., "Derecho penal argentino", t. 4, p. 208, N° 67 y CARNELUTTI, F., "Studdi sulle energie come ogetti de rapporti giuridici", Rivista di Diritto Commerciale, 1913, 1ª parte, p. 382. Citados por BORDA, Guillermo en ob. citada.

(24)JA, 1991-III-87, CNCrim. y Correc., sala I, 23/11/90, "T., G. E."

(25)CNCrim. y Correc., sala I, "Dubin, Isaac" (Boletín Interno de Jurisprudencia N° 3, año 1991, mayo-junio).

(26)En tal sentido apunta la tesis de Pierre Catalá, sobre propiedad de la información ("Ebauche d'une théorie juridique de l'information", Recueil Dalloz Sirey, 16° cahier, Chronique, 1984) citada y resumida por CORREA, Carlos M., en "Derecho informático", ps. 287 y sigts., Ed. Depalma, 1987.

(27)SOLER ob. cit., t. III, p. 468.

(28)LA LEY, 1990-C, 265, CNCrim. y Correc., sala IV, febrero 13-990, "Oliva, Jorge".

(29)NUÑEZ, "Derecho penal", t. V, p. 537.

(30)NUÑEZ, "Derecho penal", t. V, p. 533.

(31)CNCrim. y Correc., sala V, abril 29-991, "Chapman, Ricardo", LA LEY, 1991-E, 658.

(32)NUÑEZ, "Derecho penal", t. V, p. 537. En la nota Núñez cita a Goizard, t. VIII, p. 251 y BORDA, Ernesto Eduardo, Enciclopedia Jurídica Omeba, t. I, p. 765.

(33)NUÑEZ, "Derecho Penal", t. V, p. 538.

(34)"Booteo" es el proceso por el cual la computadora se enciende.

(35)Véase la revista Facetas, 1989, Fred Cohen es profesor de ingeniería eléctrica y de computación en la Universidad de Cincinnati, Ohio. Es autor de numerosos artículos sobre la lucha contra los virus en las

computadoras.

(36) SOLER, Derecho Penal Argentino, t. IV, p. 480.

(37) André Bertrand es Director del CIREDIT (Centre International de Recherches et d'études du Droit de l'Informatique et des Telecommunicatios) y profesor en la Universidad París I, Francia.

(38) Si bien la doctrina no es coincidente acerca de la validez de un Derecho Penal Internacional, aceptan la existencia de simples recomendaciones dirigidas a los Estados, para que promulguen determinados preceptos penales (JESCHECK, H. H., "Tratado de Derecho Penal", t. I, p. 165 y sus citas, Ed. Bosch, Barcelona). Sin embargo en la clasificación que realiza el autor de las normas penales de carácter internacional no encontramos ninguna que se adecue a los hechos descritos en esta nota.