Aspectos legales de los virus informáticos

JULIO TÉLLEZ VALDÉS
Doctor en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier I
Investigador en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.
(MEXICO)

SUMARIO

I. GENERALIDADES

El virus informático, aunque difícil de conceptualizar dada su misma naturaleza técnica a pesar de ser una expresión con inevitables recubrimientos científicos derivados de la acepción «virus», se ha considerado como un pro-

grama que puede infectar a otros, modificándolos para incluirles una copia ejecutable de sí mismo o cambiar parte del código.

El virus puede extenderse cuando el usuario hace uso de el programa contagiado, infectando a otros discos y programas.

La mayoría de los virus no dejan señales externas de su presencia despues de infectar; un programa infectado puede operar normalmente por cuatro meses o hasta ocho años sin dar señal de alguna infección.

Durante este tiempo el virus se reproduce calladamente en otros programas del sistema operativo y en diskettes insertados en la computadora. Después de un período de reproducción el virus se activa, entonces se manifiesta el disturbio que tiene el sistema, ya sea con mensajes, con la aparicion de figuras flotantes, o bien, puede causar una parcial o total destrucción de información almacenada.

Estos virus, en la mayoría de las ocasiones se introducen en las computadoras con motivo del uso indebido de algún equipo o programa, provocando desde la interrupción de las sesiones de trabajo y la pérdida de datos o archivos en los medios de almacenamiento de información, hasta daños al propio sistema. Son «programas» reducidos que en pocas líneas contienen instrucciones, parámetros, contadores de tiempo o del número de copias, mensajes, etc.; casi nunca incluyen el nombre del autor, ni el registro ni la fecha, reproduciéndose a sí mismos y tomando el control o modificando otros programas.

La Computer Virus Industry Association, integrada por compañías y programadores que desarrollan programas destinados a la prevención, detección y erradicación de virus, ha agrupado a estos en tres clases distintas: infectores del área de carga inicial (boot infectors), infectores del sistema e infectores de programas ejecutables (extensión com o exe):

a) Infectores de carga inicial: infectan los diskettes o el disco duro, alojandose inmediatamente en el área de carga, o sea, en el sector 0. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo. Aún en caso de reinicialización del ordenador, el virus permanece en el sistema e infecta el disco inmediatamente si este no esta protegido contra escritura.

b) Infectores del sistema: se introducen en los programas del sistema, por ejemplo, el command.Com y otros que se alojan como residentes en memoria. Los comandos del dos, como COPY, DIR o ERASE, son programas que se introducen en la memoria al cargar el sistema operativo y es asi como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver su directorio.

c) Infectores de programas ejecutables: estos son los virus más peligrosos ya que se diseminan fácilmente hacia cualquier programa como es el caso de las hojas de cálculo, juegos, procesadores de textos, etc. La infección se produce al ejecutar el programa que contiene el virus que en ese momento

se posiciona en la memoria de la computadora y a partir de entonces infectará todos los programas cuya extensión sea .Exe o .Com en el instante de ejecutarlos a fin de invadirlos autocopiándose en ellos. Esta operación pasará inadvertida para el usuario, pues sólo vera que la luz de la unidad de disco esta encendida, lo cual indica que se esta cargando el programa. Aunque la mayoría de estos virus ejecutables «marca» con un byte especial los programas infectados para no volver a realizar el proceso en el mismo disco, algunos de ellos se duplican tantas veces en el mismo programa y en el mismo disco, que llegan a saturar su capacidad de almacenamiento.

A más de la gran cantidad de elementos técnicos en torno a este problema, de los cuales hemos señalado algunos de los más esenciales, cabe mencionar que bajo una perspectiva económica, el tema de los virus informáticos constituye una paradoja muy singular, ya que si bien por un lado generan pérdidas económicas sustanciosas a las empresas o particulares usuarios de informática afectados por los virus, por el otro lado son varias las compañías que «capitalizan» la situación a través de las ganancias generadas con motivo de la venta de los cada vez más famosos «antivirus».

II. ORIGEN DEL VIRUS:

Se considera al virus computacional como un problema de la década de los 80's, pero la idea del virus nació desde los años 50's con la teoría de John Von Newmann, en la que hablaba de que los programas del computador podrían multiplicarse de forma alarmante; posteriormente un grupo de científicos le dieron vida a esta teoría y asi crearon «la guerra de memoria», esta fue inspirada en un programa escrito en ensamblador llamado «Creeper», el cual podía duplicarse cada vez que este corría. Para contrarestarlo, fue creado el programa «REEPER», cuya función fue la de destruir cada copia hecha por CREEPER, y autodestruirse cuando ya no existiera ningún «CREEPER».

III. CAUSAS:

Investigaciones recientes llevadas a cabo en los Estados Unidos, indican que un 70% de los virus existentes fueron realizados por personal interno y autorizado de las propias empresas. El otro 30% que es el medio mas común de contagio, son programas que entran a las instalaciones por primera vez, en copias de programas no originales.

Las tres principales causas por las que se crearon estos virus son:

1) Empleados descontentos.

2) Programadores interesados en rebasar los limites de las más reciente tecnología.

3) Empresas interesadas en la piratería de software.

IV. TIPOS DE VIRUS:

Entre las diferentes variedades de virus mas importantes conocidos hasta ahora, con especial incidencia en los equipos IBM o compatibles, tenemos, en estricto orden alfabético, los siguientes:

* AIDS también conocido como HAHAHA, MOFA y VGA2CGA
* ALABAMA
* ALAMEDA también conocido como MERRIT, PEKING, SEUL y YALE
* AMSTRAD
* ASHAR también conocido como SHOE VIRUS y VIRUS UIUC
* CASCADE también conocido como OTOÑO, LETRAS CAIDAS, 1701 y 1704
* CASCADE B también conocido como BLACKJACK y 1704-B
* BRAIN también conocido como CEREBRO PAKISTANI
* CHAOS
* DARK AVENGER
* DATACRIME también conocido como 1280 o DIA DE COLON
* DATACRIME II también conocido como 1514
* DATACRIME IIB también conocido como 1917
* DATACRIME B también conocido como 1168
* DBASE
* DEN ZUK también conocido como BUSQUEDA o VENEZOLANO
* DEVIL'S DANCE también conocido como MEXICANO
* DISK KILLER también conocido como OGRO INFORMATICO u OGRO DEL DISCO
* DO NOTHING VIRUS también conocido como VIRUS ESTUPIDO
* EDV
* FRIDAY THE 13TH COM virus también conocido como VIRUS .COM, MIAMI, MUNICH, SUDAFRICANO o VIRUS 512
* FUMANCHU también conocido como 2080 y 2086
* GHOST BOOT
* GOLDEN GATE también conocido como MAZATLAN o VIRUS 500
* HALLOPECHEN
* HOLLAND GIRL también conocido como SYLVIA
* ICELANDIC (existen 3 versiones) también conocido como CERO DE CADA DIEZ o CRUJIDOR DE DISCOS
* JERUSALEM (también 3 versiones) conocido como PLO, ISRAELI, VIERNES 13, RUSO, 1813 (COM) o 1808 (EXE)
* JOKER
* LEHIGH
* LISBON
* MIX/1

* OHIO
* OROPAX también conocido como VIRUS DE LA MUSICA
* PAYDAY
* PENTAGON
* PERFUME ALIAS 765 o 4711
* PING PONG (dos versiones) también conocido como TURIN o VERACRUZ
* SARATOGA también conocido como 642 o UNO DE CADA DOS
* SF VIRUS
* STONED tambien conocido como HAWAI, MARIGUANA, NUEVA ZELANDIA, SAN DIEGO o SMITSONIANO
* SUNDAY
* SURIV (tres versiones)
* SWAP
* SYSLOCK también conocido como 3551 o 3555
* TAIWAN
* TRACEBACK (dos versiones) tambien conocido 3066
* TYPO BOOT
* TYPO COM también conocido como TANTEO u 867
* VACSINA
* VCOMM
* VIENNA (dos versiones) también conocido como AUSTRIACO, UNESCO, DOS-62, DOS-68, 1 de 8 y 648
* VIRUS-90
* VIRUS-101
* W-13
* YANKEE DOODLE
* ZERO BUG también conocido como PALETA o 1536
* 405
* 512
* 1260
* 1559
* 1704 FORMAT
* 4096

V. EFECTOS DE LOS VIRUS:

Entre los efectos que producen los virus encontramos:

– cambia el nombre del volumen del disco,

– crea sectores malos en áreas no usadas del disco, disminuyendo paulatinamente su capacidad,

– interfieren con la operación de programas residentes en memoria RAM,

– infecta el sistema operativo,

– eventualmente cancela el BOOT y FAT (tabla de asignación de archivos) y sectores del directorio,

– provoca imágenes molestas en el monitor o envía mensajes,

– bloquea buffers de manera que no permite la entrada o salida de los discos, pareciendo una falla de software,

– daña físicamente a la computadora.

De lo anterior se desprenden dos aspectos: uno positivo ya que ahora los usuarios saben que tienen que ser mas cuidadosos y no hacer copias indiscriminadas de paquetes o discos respetando así los derechos de autor, también ahora los usuarios que han perdido toda o parte de su información debido a un virus, saben que es una práctica muy sana hacer respaldos periódicos de su información, asegurando así que la mayoría de la información estará a salvo. El aspecto negativo es el miedo al contagio de virus, evitando el intercambio de información importante que antes era fomentada, ocasionando con esto pérdida de tiempo y dinero.

VI. MEDIDAS PREVENTIVAS:

Para evitar el contagio de virus es importante:

– utilizar paquetes originales,

– tener un control de las claves de acceso,

– proteger los diskettes así como los discos duros,

– elaborar contratos laborales en las empresas contra el mal uso de los paquetes,

– tener un control de los equipos,

– realizar auditorías internas,

– programa que impide la inserción de programas «contaminados».

VII. MEDIDAS CORRECTIVAS:

El virus es una amenaza potencial a la integridad del software de cualquier computadora, debido a este problema se han creado un nuevo tipo de software «las vacunas» cuya función es detectar y eliminar el virus del disco recuperando en algunos casos la información del mismo y evitando que siga infectando otros discos.

Mas es importante tener presente que no es posible escribir un programa que detecte todos los virus concebibles, es posible construir una defensa contra cualquier virus dado y para cada defensa siempre habrá otro virus que pueda burlarla.

VIII. SEGURIDAD EN LOS CENTROS DE COMPUTO

La seguridad en centros de cómputo tiene por objeto la protección de los intereses de una organización salvaguardando el equipo, sus programas y

los datos, asegurando asi la operación confiable e ininterrumpida del sistema de cómputo.

Los especialistas en seguridad para computadoras identifican cuatro niveles o capas en la proteccion del software y el hardware.

El primer nivel, «electrónica y programación», se refiere a la protección proporcionada por los dispositivos del hardware y por las técnicas de software con que hayan sido provistos el sistema operativo, los archivos de datos y los programas de aplicación.

El segundo nivel, «protección física», corresponde por una parte a las medidas de seguridad contra incendio y fenómenos naturales y por otra, a los mecanismos que impiden el acceso al centro de cómputo y lo protegen contra atentados y robo. Asimismo, incluye a todos los procedimientos para hacer frente a contigencias.

El tercer nivel, «políticas de la organización», está constituido por los métodos y procedimientos administrativos desarrollados por la organización, en los cuales se ve involucrado el centro de cómputo.

El cuarto nivel «controles legales», consiste en la protección otorgada por las leyes internacionales, nacionales y locales y considera también los convencionalismos aceptados por la sociedad de que se trate.

La seguridad absoluta es prácticamente imposible de alcanzar en los cuatro niveles y esto se debe a la gran cantidad de elementos que componen al problema. Siendo realistas, lo que normalmente se busca al planear un sistema de seguridad es:

– minimizar la probabilidad de una falla de seguridad o una pérdida de información y,

– minimizar el daño que pudiera resultar de ellas.

El virus se manifiesta al poner en marcha el programa portador, burlando el primer nivel de seguridad. Aquí la prevención, detención y eliminación del virus corre principalmente por cuenta de programas antivirus o vacunas, aunque también es posible proteger físicamente contra escritura a algunos discos.

En el caso de destrucción de información por un virus son los procedimientos de respaldo del centro de computo, en el segundo nivel de protección, los que garantizan el restablecimiento de la información en las condiciones en que se encontraba antes de la falla.

Si bien es probable que los respaldos también están contaminados, pueden servir para rastrear, aislar y eliminar en ellos al virus.

Las medidas preventivas mas eficaces se toman generalmente en el tercer nivel de protección, donde se puede establecer una cuidadosa política para el uso de programas comerciales y del dominio público y para la conexión a redes de computadoras y centros de información electrónicos.

Todas estas acciones y otras similares brindan protección de los efectos de los virus que ingresan al sistema al intercambiar discos o recibir información por vía telefónica. Pero debe hacerse notar que los virus mas peligrosos son los de creación local, es decir, los desarrollados por los programadores del sistema. Ciertamente no son muy comunes pero representan el verdadero origen del problema y si de una vez por todas se pretendiera acabar con el, es en este punto donde deberían concentrarse los esfuerzos de prevención.

IX. ELEMENTOS JURIDICOS

Toca en turno hablar de las consideraciones legales en torno al problema de los virus informáticos. Para ello, es menester mencionar que dicha problemática a pesar de sus inevitables orígenes técnicos, tiene una connotación eminentemente económica que motiva a su vez la tutela por parte del derecho. Esto es que la pérdida o modificación de la información (o aún del sistema mismo) con motivo de la aparición de un virus informático, genera evidentemente pérdidas en lo económico (desde luego si no se cuentan con archivos de respaldo o alguna otra protección) de las cuales cabe determinar responsabilidades y hacer éstas exigibles.

Uno de los aspectos fundamentales aún no resueltos es el de regular jurídicamente la información considerada ésta como un bien intangible o inmaterial con un contenido económico intrínseco que radica en la destinación de que puede ser objeto. A falta de esto, se ha tenido que recurrir a cuestiones análogas tales como los contratos a través de cláusulas de secrecía y confidencialidad tanto en el caso de los empleados informáticos como con los proveedores de bienes y servicios informáticos.

Si bien la pérdida de información en estas condiciones puede considerarse como un riesgo informático, susceptible de eventual aseguramiento, cabe mencionar la prácticamente nula cobertura en este sentido seguramente motivada por ese carácter inmaterial de la información, lo que dificulta un cabal resarcimiento en caso de daños.

Sin lugar a dudas que una de las principales causas de la aparición de los virus informáticos, es la derivada de la piratería de los programas de cómputo que al no tener una respuesta eficaz por parte del derecho, y digo eficaz porque si bien la tendencia en estos momentos es proclive hacia los derechos de autor, siguen aún los cuestionamientos sobre la aplicabilidad de figuras tales como las patentes, yo mantengo mi parecer en el sentido de la necesaria emanación de una institución jurídica nueva totalmente particularizada, pues bien retomando la premisa inicial, es esta falta de protección que ha provocado el que «algunos» creadores de software pretendan hacerse justicia «por su propia mano» al no encontrar dispositivos reales de salvaguarda de sus intereses.

El regular o intentar regular jurídicamente este problema de los virus, nos remite de manera irremisible a los llamados «delitos informaticos», ya que finalmente, al menos en mi opinión, la responsabilidad derivada en estos casos deberá ser fundamentalmente exigida a través de una responsabilidad penal y no tanto civil, que sería mas paliativo que solución. Esta «tipificación» implica una debida identificación de los requisitos «sine qua non» como serían el sujeto activo (aquel creador o propagador de virus), sujeto pasivo (persona física o legal que resiente los daños) y el bien jurídico tutelado (los datos o información perdidas o modificadas). Por otro lado, la elaboración de un perfil delictivo en la que se especifique el carácter intencional o imprudencial de la acción, así como los casos en que se causen mayores estragos de lo pretendidos en aquello que se conoce en la doctrina penal como los delitos praeterintencionales.

X. CONSIDERACIONES FINALES

Como podemos percibir, el tema de los aspectos legales de los virus informáticos es complejo, y seguramente estas líneas breves pero espero sustanciosas no contienen los elementos de solución suficientes, sin embargo, con el ánimo de no limitarme a lo meramente enunciativo es menester sugerir la necesaria regulación de este fenómeno a través de cuerpos normativos coherentes, fundamentalmente a nivel internacional que de algún modo atenúen la cada vez mas progresiva anarquía respecto a los usos inadecuados de la computadora, en buena parte motivados por una deficiente deontología informática.

COLOQUIOS