Los Virus Computacionales como medio de Protección del Software

JORGE MIER Y CONCHA SEGURA

Licenciado en Derecho, Asesor en Propiedad Industrial e Intelectual, Inversiones Extranjeras y Derecho del Trabajo.

(MEXICO)

Nadie debe asustarse de lo que piensa aunque su pensar aparezca en pugna con las leyes más elementales de la lógica.

Antonio Machado

VIRUS.–(Del Lat. Virus, Tumor, ponzoña) Bact. partícula ultramicroscópica de nucleoproteína capaz de multiplicarse en ciertas células vivas, y que produce muchas enfermedades en las plantas, los animales y el hombre.[1]

Informática. Es un fragmento de un programa de computación, usualmente unido al principio o al final de un arhivo normal de un programa, que contiene una instrucción que le permite duplicarse a sí mismo o llevar a cabo alteraciones, destrucciones o alguna acción complementaria, en archivos aislados o en discos completos.[2]

I. CUESTIONES PRELIMINARES

Pakistaní, Miguel Angel, Viernes 13, El baile del Diablo; frases, nombres, fechas, lugares, que muy posiblemente usemos a diario, sin embargo,

[1] SELECCIONES DEL READER'S DIGEST, Gran Diccionario Enciclopédico Ilustrado Tomo VIII, México, Edit. Reader's Digest México, 1972.

[2] TYLER,G. –New Technology–. Management Services, Vol. 34, No. 6, 1990, pp. 21-24.

para un programador o usuario de una computadora, su significado real va más allá de la simple literalidad.

Los virus computacionales, parte integrante de lo que comunmente se ha denominado «SOFTWARE ROGUE» (Bribón, Maleante), han logrado, actualmente, infectar por encima de 16.000 computadoras alrededor del mundo, ocasionando pérdidas materiales incalculables.

El Software Rogue, que se define como todo aquel conjunto de instrucciones o dispositivos tendientes a alterar el funcionamiento normal de un sistema computacional, surge en principio por la falta de protección que los programadores sienten de sus creaciones. Mucho antes de los casos de Look and Feel, existía el problema de la piratería, cuyos antecedentes son tan remotos como el software mismo.

La aceptación dentro de los Derechos de Autor de los programas de computación, partió de dos supuestos, el primero referido a que, para las obras autorales, se reducen significativamente los requisitos de protección, siendo simplemente la originalidad y la objetivización (fijación tangible) indispensables, y no así, como en el caso de las figuras protegidas por la Propiedad Industrial, exámenes o cuestionamientos profundos de novedad; y en segundo término, la generalización que a nivel mundial había alcanzado este sistema.

Resulta obvio que un sistema de protección implantado más por comodidad que por conveniencia, fuese superado rápidamente por los avances tecnólogicos, de ahí que, al continuarse con el copiado no autorizado de programas, sus autores buscaran medidas alternas para evitar las reproducciones ilícitas, y obtener la remuneración justa por su trabajo.

Surgieron pues, entre otros, la criptografía, los códigos de acceso, los caballos de Troya, las bombas lógicas, los gusanos y los virus, que con el correr del tiempo fueron aumentando sorpresivamente su capacidad destructiva y reproductiva.

Antecedente de los virus, lo constituye el gusano, software rogue que se caracteriza por trasladarse a través de una red de computadoras reproduciéndose en cada una de las terminales, hasta que la cantidad de memoria que ocupa es tal, que ocasiona la caída o falla del sistema. En principio, el gusano, como los virus, no traía consecuencias destructivas, sino simples molestias, o mensajes tendientes a ridiculizar al usuario por su falta de ética, pero eran fácilmente superables, pues al apagar la máquina, todo efecto desaparecía.

Sin embargo, estas advertencias no cambiaron la mentalidad de los piratas informáticos, quienes en lugar de disminuir sus actividades, las aumentaron, ¿y por qué no?, el hardware se depreciaba con velocidad, aún y cuando su capacidad crecía exponencialmente, mientras que el software aumentaba, momento a momento su valor. Un pirata, a mediados de los ochenta se jac-

taba al mostrar todo lo que había podido conseguir, desde los programas más sencillos hasta los últimos lenguajes, no importando que nunca llegara a utilizarlos, pues la filosofía era «quien más tiene, más sabe». Así, los programadores se vieron forzados a cambiar palabras por acciones, trayendo en consecuencia la malignidad de los virus.

> «Octubre 1987. Una gran cantidad de usuarios de microcomputación de la Universidad de Delaware (E.E.U.U.), han estado reportando problemas relacionados con sus discos de datos. Al mismo tiempo, usuarios del área de acceso general de microcomputación, han tenido graves problemas para correr determinados paquetes de software».
>
> «Diciembre 1987. Un usuario de una computadora personal IBM en Israel se dió cuenta que un programa que había corrido cientos de veces en el pasado, repentinamente había dejado de funcionar ya que era demasiado grande para la capacidad de memoria».

Pequeñas notas periodísticas, como estas, fueron dando aviso de pérdida de información de sistemas, a medida que el uso de los virus fue en aumento, las pequeñas notas pasaron a ser encabezados, como sucedió el pasado 6 de marzo, fecha de ataque del virus conocido como Miguel Angel, en honor del natalicio del gran artista italiano, noticia que ocupó las primeras planas Japón hasta México. Los virus se convirtieron en armas informáticas, la antigua idea de protección degeneró en un virus destructivo; crear no para defenderse, sino para atacar.

El hecho de que el software sea tan fácil de reproducirse, ha favorecido la propagación de los virus, el ingresar información vía MODEM, conectarse con una red, bajar información vía satélite, o utilizar shareware ya implica cierto riesgo de infección.

La amenaza vírica ha superado todas las fronteras, todos los lenguajes e ideologías, creciendo de tal manera, que no hay un solo usuario que aprecie sus archivos, que no tenga fobia a utilizar un programa ajeno, sin pasarlo previamente por un SCAN o bien sin haberlo «vacunado». Hasta cierto grado los virus han cumplido su función, ¡pero a que costo!.

El primer proceso criminal en que se condenó a un programador rogue, dió inicio en mayo de 1988, cuando la compañía de valores UPSA e IRA Co., ubicada en Fort Worth, Texas, Estados Unidos, demandó a su antiguo oficial de seguridad informática, Donald Gene Burleson, acusándolo de haber ingresado en los sistemas de la empresa un virus que ocasionó la pérdida de más de 168.000 registros de ventas. Se comprobó que El Sr. Burleson activó el virus, dos días antes de ser despedido, lo que le valió una condena de 7 años de prisión y pago de una indemnización a favor de la empresa de 12.000 dlls US.

A este caso siguieron varios en el mismo sentido, entre los más discutidos, pues fue el primero que transgredió las barreras estatales e ingresó al ámbito federal de justicia de Estados Unidos, el de Robert T. Morris Jr., un

universitario de 23 años, que creó un Gusano que se extendió por varias universidades americanas hasta llegar a penetrar los archivos de la NASA. Increiblemente en un lapso de 36 horas, contagió más de 6000 computadoras. El culpable, aunque actuó con negligencia, enfrentó una sentencia de 5 años de prisión y multa de $250,000 dlls US.

En ambos casos las leyes que se aplicaron tenían menos de tres años de vigencia.

La mayoría de los países latinoamericanos, en esta época de apertura de mercados, se enfrenta a un grave problema, pues los órganos judiciales carecen de la preparación suficiente para desentrañar los efectos y alcances que pueden traer consigo los delitos informáticos. El caso mexicano sirve de claro ejemplo para demostrar lo sustentado con anterioridad, pues en vísperas de la celebración del Tratado de Libre Comercio y de las reformas a la Ley de Inversiones Extranjeras, la apertura económica y el ingreso de capitales frescos del exterior se hace inminente. No obstante, la euforia de su firma nos hace olvidar los problemas legales que enfrentaremos, sobre todo con los Estados Unidos de América, pues su sistema legal, mucho más flexible que el nuestro, plantea serias penas, como ya se mencionó, a algunos delitos informáticos, mismos que las leyes mexicanas ignoran. Dentro de las bases que conforman el Tratado Trilateral de Referencia, se establece una especial protección a las figuras que contemplan los derechos intelectuales, muy particularmente a los programas de cómputo y circuitos integrados, manteniendo, sin embargo, a los primeros en el ámbito de protección autoral.

Abordaré el problema de los virus desde diferentes puntos de vista, a fin de poder tener una visión global del problema, a sabida cuenta que los factores sociales y económicos no se separan jamás del derecho, pues este es resultado de la realidad en que se vive, del Aquí y Ahora.

II. DESDE EL PUNTO DE VISTA DEL DERECHO DE AUTOR

¿Qué pasa con los virus en la legislación mexicana?. La Constitución Política de los Estados Unidos Mexicanos, consagra el Derecho de Autor, en su artículo 28 al decir:

> «...Tampoco constituyen monopolios los privilegios que por determinado tiempo se concedan a los autores y artistas para la producción de sus obras y los que para el uso exclusivo de sus inventos, se otorguen a los inventores y perfeccionadores de alguna mejora».

El artículo séptimo de la misma regulación, añade que:

> «...Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública...».

El art. 19 de la Ley Federal de Derechos de Autor vigente, complementa los artículos anteriormente citados al decir:

«El registro de una obra intelectual o artística no podrá negarse ni suspenderse bajo el supuesto de ser contraria a la moral, al respeto a la vida privada o al orden público, sino por sentencia judicial, pero si la obra contraviene las disposiciones del código penal o las contenidas en la Convención para la Represión del Tráfico y Circulación de Publicaciones Obscenas, la Dirección General del Derecho de Autor lo hará del conocimiento del Ministerio Público para que proceda conforme a la ley».

De la lectura de los preceptos anteriores, se desprende que los virus, independientemente de su finalidad o función, por el solo hecho de ser obras se encuentran bajo la tutela del Derecho de autor.

III. DESDE EL PUNTO DE VISTA DEL DERECHO PENAL

Un enorme problema radica en que, un gran porcentaje de las legislaciones mundiales, no contemplan dentro de sus códigos respectivos a los delitos informáticos, siendo, hasta el año pasado, los más actualizados, los países del Common Law o Derecho Común. A pesar de ello, basándose en el viejo principio de derecho penal que dice: *«Nullum crimen, nulla poena sine lege»,* poco se ha podido hacer, ya que por más que se intente identificar ciertas conductas informáticas consideradas ilícitas con delitos previamente establecidos, queda al ánimo del juzgador la decisión final.

Analicemos tres de los casos, que, muy posiblemente lleguen a tribunales en relación con los virus, para que una vez expuestos podamos, a la luz del derecho, concretizar sobre el beneficio o perjuicio de los mismos.

Desde el punto de vista del programador, creador del virus, el mismo es sujeto de protección, más aún si se encuentra contenido en un programa aplicativo o en un sistema y, permanece inactivo en tanto no se realice una copia ilegal, puesto que la única copia que se autoriza al tenedor de un programa de computación es la de respaldo o backup (artículo 18 Ley Federal de Derechos de Autor). En consecuencia, cualquier otra copia con fines de lucro le valdrá una pena de 6 meses a 6 años de prisión y multa de 50 a 500 veces el salario mínimo (art. 135 de la misma Ley). Es de conocimiento general, que es prácticamente imposible el detectar a un trangresor del art. 135 citado, es en consecuencia, el virus, el medio eficaz para encontrar al culpable. En este orden de ideas, el copista que transgredió la ley, debe entonces, para liberarse del virus, contactar a la compañía distribuidora o bien al programador, para solicitar una vacuna o antídoto, previo registro como usuario autorizado, con todas las ventajas que se confieren como tal, por ejemplo el manual de operaciones, y la asistencia técnica. Hipotéticamente estas medidas diminuyen los casos de piratería autoral del software.

Segundo caso, supongamos que un virus creado con el solo propósito de protección, resulta ser mucho mas dañino de lo esperado, como le sucedió al Sr. Robert T. Morris Jr., y provoca cuantiosas pérdidas de información y programas ajenos; cierto es que, la propagación del virus derivó de una con-

ducta ilícita, pero también que, debido a una imprudencia del programador rogue, se ocasionaron cuantiosas pérdidas materiales, muy desproporcionadas a la simple copia del programa.

Tercer caso, en una actitud ciento por ciento dolosa, un programador rogue crea un virus «maligno» con el solo propósito de dañar los programas o sistemas de algún particular, sociedad o del público en general, podemos entonces afirmar que, se está atentando ya, contra la vida privada, violando el orden social, y en consecuencia incurriendo en una conducta ilícita.

Dice el Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, que los Derechos de Autor se consideran bienes muebles (art.758), siéndole por tanto, aplicables las disposiciones relativas a los mismos. Tomando en consideración lo anterior, considero que dentro del Código Penal del D.F., existe sólo un delito por el cual se puede inculpar a un programador rogue: EL DAÑO EN PROPIEDAD AJENA. Este delito se define en los siguientes términos:

> «Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena o de propia en perjuicio de tercero».

La penalidad establecida va desde los 2 a los 10 años de prisión, y multa de 100 a 500 veces el salario mínimo, segun la cuantía de lo dañado.

Estas podrían ser las sanciones a aplicar en el tercer caso hipotético visto anteriormente. Sin embargo, si la conducta del programador fue preterintencional, es decir, cuando se cause un resultado típico mayor al querido o aceptado, si aquel se produce por imprudencia (segundo caso), la pena se podrá reducir hasta una cuarta parte. Por otro lado, si el delito resultare ser totalmente imprudencial, esto es, se realiza un hecho típico incumpliendo un deber de cuidado, la pena sería de 2 días a 5 años de prisión.

Es sumamente difícil, desde el punto de vista jurídico-procesal, comprobar que alguien, a través de un virus, causó daño en propiedad de un tercero. Hace falta definitivamente, una regulación especializada que no se preste a excesos, y que regule especificamente estos delitos, para evitar confusiones e injusticia.

Si por cualquier motivo, estos virus llegaran a causar delitos superiores a la pérdida de información, me refiero especialmente a aquellos que afecten la vida o la integridad física de las personas, como estuvo a punto de ocurrir con el virus conocido como «SIDA», ¿qué decidirán los tribunales?. Relatare brevemente el caso:

Marzo 1989, diversos hospitales a lo largo de Europa, encuentran sus sistemas de registro y datos personales de pacientes, invadidos por un virus que deplegaba en pantalla un mensaje, informando que la computadora estaba infectada y que, para regresarla a la normalidad, debía mandarse un «donativo» a cierta dirección en Panamá; cómo este virus ponía en peligro la vida de pacientes, aunque los hospitales después se empeñaron en negarlo, di-

ciendo que sólo se trataba de un virus «benigno», se decidió que en vez de seguir un proceso legal de dudosos resultados, era más práctico, y menos riesgoso para ellos, contribuir con el donativo y recibir vía aérea la vacuna.

Un maestro de derecho penal, nos decía en sus clases, que la mente del delincuente, va un paso adelante de la del legislador, ya que este último regula y sanciona y el delincuente actúa para escapar de la aplicación de esa ley.

Los delitos informáticos son variados, desde los famosos «Hackers», ingreso a información confidencial, modificación de archivos, hasta el terrorismo informático. Las desastrosas consecuencias económicas o sociales no se ponen en duda, y de ello deriva la necesidad de un legislación penal actualizada que regule estas conductas claramente ilícitas.

Basta concluir que, independientemente de que la pena que la Ley Federal de Derechos de Autor mexicana señala para el caso de copia no autorizada de algún programa (piratería), es correcta, en la mayoría de los casos es letra muerta, por lo que para reducir los delitos negligentes o imprudenciales derivados de los virus, se debe primero aplicar de modo estricto dicha ley.

IV. DESDE EL PUNTO DE VISTA DEL DERECHO CIVIL

A la luz de lo ya analizado, puedo afirmar que, en relación con los efectos de los virus, en una demanda civil contra un programador rogue, para su procedencia, se requiere acreditar el derecho de autor violado o bien la propiedad de la información destruida por el virus.

Dos problemas se derivan de lo anterior, el primero se refiere al hecho de que la Ley Autoral consagra el Pricipio de Protección Automática, principio que trae como resultado que muchos programadores no registren sus creaciones y, el segundo, que la información utilizada por grandes empresas o personas a diario, NO ES OBJETO DE REGISTRO, en virtud de lo complicado que resultaría hacerlo, aunado a que dicha información puede cambiar de un momento a otro. De ello deriva que el demandar civilmente por daños y perjuicios, procederá sólo en el caso en que se logre comprobar la existencia y legal propiedad de la información y/o programas afectados, pruebas que en la práctica serán cubiertas por muy pocas personas, debido al desconocimiento de tales requisitos para acreditar la referida propiedad y, de que ninguna ley contempla disposiciones claras y objetivas en cuanto a pérdida de información, ya que únicamente se refiere al registro o no de los programas.

Un medio por el que civilmente, los usuarios podrían cubrirse del riesgo de perder su informacion, es la contratación de seguros, donde, en caso de siniestro, la empresa aseguradora pagaría los daños, subrogándose a su vez en nuestro derecho de demandar al creador del virus. En Estados Unidos, se ha comenzado ya a otorgar pólizas de este tipo, con muchas limitaciones y lagunas, pero cobertura al fin y al cabo.

V. INFLUENCIA INTERNACIONAL

Es conveniente antes de cerrar este estudio, hablar acerca de la tendencia que a la fecha esta tomándose en Europa, a raíz de la Propuesta de Directiva de Programas de Ordenador de la Comunidad Económica Europea, ya que tendrá seguramente, gran influencia futura en los criterios de los juzgadores en todo el mundo. Quiero referirme especialmente al articulo 7o. de dicha propuesta, que a la letra menciona:

«...Art. 7. Medidas especiales de proteccion:

1. Sin perjuicio de las disposiciones de los arts. 4, 5 y 6, los Estados miembros, de conformidad con sus legislaciones nacionales, deberán adoptar medidas adecuads contra las personas que cometan cualquiera de los actos mencionados en las letras siguientes:

a...

b...

c. La puesta en circulación o tenencia con fines comerciales de cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador.»

2...

3. Los Estados miembros podrán ordenar la confiscación de los medios a que hace referencia la letra c del apartado 1.

En una primera lectura, se entiende que las vacunas son un medio de eliminar dispositivos técnicos de protección, el hecho es que, si queremos copiar un programa que sabemos está protegido por un virus, estamos cometiendo el delito de reproducción no autorizada y, en consecuencia, la utilización de una vacuna esta prohibida, aún y cuando la finalidad con la que se utilice NO SEA COMERCIAL. Ahora bien, suponiendo que el virus es ajeno a nosotros, y que se transmitió a través de una red o de comunicación vía satélite, y se usa la vacuna para desinfectar nuestros programas infectados, materialmente no estaríamos sujetos a la aplicación del punto uno del artículo citado, pero si la autoridad requiere que se entreguen las vacunas, como se contempla en el punto 3, deberá hacerse y, en consecuencia, ¿cómo van a cubrirse los usuarios?.

No se toma en cuenta tampoco, que hay casos en los que son los mismos programadores quienes incluyen en sus creaciones los virus, a efecto de poder después transmitir las vacunas, creadas también por ellos, mediante previa «donación», excluyéndose así, del ámbito de aplicación de dicha norma, puesto que repito, no tendría una finalidad comercial ya que que no se está vendiendo, sino solicitando opcionalmente una ayuda altruista para continuar con sus investigaciones.

El documento que se analiza, no menciona nada al respecto de la pérdida de información derivada de la programación rogue, ni de hasta qué grado los dispositivos técnicos de protección son o no lícitos.

A mi punto de vista deberían de especificarse los dispositivos a los que se refiere, puesto que si los mismos se usan para proteger información confidencial, estoy de acuerdo en la supresión de los medios que los eliminen, por otro lado, si se contempla a los virus, este precepto no es de tan lógica aplicación.

Evidentemente, las vacunas no deben ser estrictamente prohibidas, como tampoco lo deben ser los virus, pero es de tener siempre en cuenta que somos una comunidad, y como tal, nuestro derecho llega hasta donde empieza el derecho ajeno.

VI. CONSIDERACIONES FINALES.

Se ha repetido hasta el cansancio que la única manera de acabar con los virus es reduciendo el riesgo de contagio, evitar introducir paquetes de dudoso origen, realizar continuamente revisiones de los discos, reportar oportunamente cualquier irregularidad, etc. Es cierto que estas acciones pueden minimizar el peligro, pero no lo erradican. El problema entonces, se centra en determinar si los virus y las vacunas deben ser reguladas o prohibidas.

Desde el punto de vista ético, quizá los virus no sean el medio idóneo para buscar la protección de un programa, pues al activarse es posible que cause daño tanto en la parte material, como en la inmaterial de un sistema de cómputo. Por otro lado, si un virus está diseñado para evitar la reproducción ilícita de un programa, el aplicar una vacuna para suprimirlo implica ya en sí, una conducta ilícita. La contraposicion de ambas ideas es evidente.

Si toda la gente se guiara por normas éticas tan sencillas como el respeto al derecho de terceros, las leyes no tendrían razón de ser, sin embargo, como humanos que somos, estamos repletos de pasiones y errores, unos más que otros, pero al fin y al cabo somos todos iguales.

Como manifesté antes, cada persona tiene derecho a proteger lo que es suyo, siempre y cuando no se violen los derechos ajenos. Hablando de virus, no se debe ser tan duro en contra de quienes buscan una protección real para sus creaciones, protección que obviamente no ha conseguido otorgar el Derecho de Autor. Si se quiere atajar un mal, se debe empezar por sus raíces, y después por sus ramas, de tal manera resulta indispensable, no sólo combatir la piratería, sino comenzar por proteger debidamente el software, regulándolo de manera global. Por esto último, me refiero a todos los aspectos del derecho, desde cómo otorgar protección hasta la especificación de las penas provenientes de conductas que puedan ser consideradas como ilícitas, en pocas palabras, una codificación informática que pueda sentar las pautas y crite-

rios base para evitar el robo, copiado no autorizado, pérdida de información propiedad de terceros, etc.

No se pueden atacar los virus como si fueran el némesis de todo programador, tomando en cuenta que fuimos nosotros mismos quienes provocamos su generación, tampoco es conveniente prohibir que se inventen medios para defendernos y mucho menos venderlos, puesto que su creación misma ya implicó cierto esfuerzo intelectual, que por justicia social debe ser remunerado; pero seamos realistas, hay un gran porcentaje de virus informáticos que se crean con el solo fin de perturbar la paz, por demostrar las habilidades de un programador, o por simple venganza, son esos virus los que deben de ser penados; el dolo, la mala fe, el ánimus de la creación es la que marca la diferencia entre defensa y ataque, porque estoy seguro que si elaboramos una base firme de protección del software, una gran parte de los virus, sobre todo aquéllos que por negligencia o preterintención se han propagado desorbitadamente, desaparecerían.