"*Una cuestión que parece moderna (los virus informáticos) pero que ya lleva más de dos décadas de debate aun no ha recibido una respuesta legislativa adecuada en nuestro medio. Mientras tanto, los virus siguen haciendo estragos en las herramientas que a diario usamos para trabajar*".

Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado

*Pablo A. Palazzi**

Resumen

1. Concepto y evolución de los virus informáticos. 2. Aplicación del Código Penal argentino a los virus informáticos. 3. Necesidad de tipificar el delito de daño informatico y el de creación o difusión de virus informático. 4. Los virus informáticos como protección de la propiedad intelectual y los negocios contractuales. 5. Responsabilidad civil por la propagacion de un virus informatico. 6. Legislación sobre daño informatico y virus en el derecho comparado. 7. Conclusiones. Bibliografía.

PALABRAS CLAVE: Virus informático. Daño. Informática. Internet. Interrupción de comunicaciones. Derecho comparado. Argentina. Ciberdelito.

Abstract

El autor examina la aplicación de las normas del código penal argentino al accionar de un virus informático.

KEYWORDS: Computer virus. Crime. Internet. Damage.

The author analyzes the applicability of the criminal laws of argentina to computer virus actions.

* Abogado (UCA y NY State Bar Assoc) y LLM en Fordham University Law School. Se ha especalizado en derecho y nuevas tecnologías de la información. Ha escrito sobre esta materia numerosos artículos y varios libros. Fundador del Foro de Habeas Data y Protección de Datos Personales. Agente de Propiedad Industrial. Profesor Facultad de Derecho Universidad Austral de Argentina. Consejero Centro de la Propiedad Intelectual de la Universidad Austral. Ex Secretario Letrado de la Corte Suprema de Justicia de la Nación. Fundador de la Revista Derecho y Nuevas Tecnologías. e-mail: p.palazzi@cekd.com - pablo.palazzi@gmail.com

1. Concepto y evolución de los virus informáticos.

Un virus informático no es un organismo con vida propia, a pesar de la analogía que presentan con los virus biológicos: ambos se reproducen engañando el metabolismo del huésped al que infectan; este proceso produce alteraciones en el metabolismo del cuerpo (o en el funcionamiento de la computadora); pueden llegar a tener un tiempo de incubación y finalmente desarrollan su efecto final. En el caso de los virus informáticos este efecto suele ser la destrucción o borrado de las memorias, tanto magnéticas como electrónicas de la misma, o la alteración del normal funcionamiento del sistema.

Un virus de ordenador es un programa que tiene la capacidad de hacer copias de si mismo en otras computadoras y producir un efecto determinado por su autor, que puede ser inofensivo o dañino. (aunque este último suele ser el efecto en la mayoría de los casos). Un virus funciona infectando el sistema operativo de la computadora. De esta manera, puede controlar todas las operaciones que realiza el ordenador. Si entre las instrucciones de este sistema operativo se inserta subrepticiamente un grupo de ordenes que hagan funcionar a la computadora correctamente, pero que llegada cierta fecha o sucedido determinado hecho activa una rutina que destruye la información de la memoria, disquete o disco rígido, estaremos en presencia de un virus informático.

Los virus informáticos no son ninguna novedad. Surgieron hace mucho en la teoría pero no tienen mas de algunos años en la práctica. Ya en 1949 John von Newmann, brillante matemático húngaro de su época, publica un artículo llamado "Theory and organization of Complicated Automata"[1] donde expone la idea de un programa que se reproduce y por lo tanto esta vivo. Seis años mas tarde, en su libro "The Computer and the Brain" hace una disertación teórica sobre la posibilidad de crear un autómata capaz de reproducirse a si mismo[2].

En la década del 60 los virus comenzaron a cobrar vida, cuando en los Laboratorios Bell, con la idea de hacer un juego surge el programa Core-War[3]. En 1983, Ken Thompson, uno de los autores de la versión original del sistema operativo UNIX, en un congreso informático reveló la existencia de esta clase de programas e instó a desarrollarlos, alegando que para ello se requerían sólidos conocimientos de programación. Muchos programadores decidieron afrontar el desafío...y lo hi-

1 Ver texto completo de la obra en http://www.walenz.org/vonNeumann/

2 Ver http://www.zyvex.com/nanotech/vonNeumann.html

3 Este software consistía en la existencia de dos programas dentro del mismo ordenador que competían por la subsistencia y dominio del computador destruyendo a sus adversarios. Era realizado por los programadores que debían quedarse a la noche trabajando y con el objeto de no "aburrirse" inventaron este juego. Estos ingenieros en sistemas habían decidido no dar a conocer la manera de realizar estos programas por el peligro que significaban.

cieron con éxito. Al despuntar 1985, la revista *Scientific American* recogía los lamentos de Richard Skrenta, estudiante de secundaria de Pittsburg cuya creación (un virus para la computadora *Apple*) había corrompido no solo los diskettes de su casa, sino también los de su escuela y consecuentemente los de todos sus compañeros. Reconocía haber desarrollado un antídoto mucho menos eficaz que el virus de su propia autoría[4].

En la edición del 28 de junio de 1988, la revista norteamericana PC Magazine publicó un reporte en el cual citaba alguno de los casos mas interesantes y también, más desastrosos de la industria. Los escépticos insistían en que la alarma producida por los virus estaba sobredimensionada, basándose en que se trataba de informaciones no confirmadas, imposibles de rastrear. La revista en cuestión, mencionaba casos como la introducción de un virus que había penetrado y virtualmente "apagado" el sistema computacional de defensa israelí; o uno que infectó el centro de computación de la universidad de Lehigh; también el virus Brain, que atacó a los ordenadores compatibles con IBM y el Scores que atacó a las computadoras Macintosh de la Universidad de Miami; también el Scores afectó a la enorme firma de computación EDS (una subsidiaria de la General Motors), la que, justamente, garantiza —como uno de sus servicios—, la seguridad de los datos de sus clientes.

Desde 1987 hicieron su aparición los primeros virus mas conocidos (Jerusalém —llamado así porque fue descubierto en los ordenadores de la Universidad homónima—, el Virus Brain, Datacrime, Datacrime II, Datacrime IIB y numerosos otros). Estos primeros virus causaron pérdidas millonarias. A estas alturas nadie podía ignorar los acontecimientos. Los virus habían dejado de ser una "diversión" o un "juego" de programadores, para transformarse en una molestia, un obstáculo para el desarrollo de la informática e incluso un delito informático.

En 1996 ya se hablaba de mas de diez mil versiones de virus distintos. Además hicieron su aparición los virus polimórficos, que tienen la capacidad de no ser detectados al mutar su código en forma aleatoria. Actualmente hay virus que atacan los telefonos celulares y las "*palms*" o agendas de bolsillo. A fines del 2003 la página de una conocida empresa antivirus señalaba la existencia de por lo menos 81.000 versiones de programas dañinos entre versiones principales, modificaciones y falsos virus, tales como los Hoax, o las cadenas de mensajes falsos. En enero de 2006, al empresa McAfee informaba de la existencia de 150.000 virus, agregando que cada mes aparecen cerca de 500 nuevos virus y amenazas a través de Internet[5].

Estos últimos años han registrado cientos de episodios de hackers y ataques relacionados con los virus, cuyo accionar obviamente se ve potenciado por

4 http://virus.dst.usb.ve/article/articleprint/34/-1/6/

5 Ver http://vil.nai.com/vil/default.asp

Internet[6]. Por ejemplo el caso del Virus Melisa, que desde Canadá infectó a ordenadores en varias partes del mundo o el caso del Virus "I Love you", que fue rastreado hasta Filipinas por el FBI. Las finalidades no son sólo de diversión. A veces contienen mensajes políticos. A fines del 2001, aparecieron varios virus que invocaban de una u otra manera a Osama ben Laden. A veces son motivados por pura maldad o intereses económicos. El virus PGPCoder, por ejemplo, se introduce en el sistema a través de una vulnerabilidad en el Internet Explorer y encripta todos los documentos (.doc y .xls), pidiendo dinero a cambio de la contraseña. El virus SoBig transforma millones de computadoras en repetidoras de spam, saturando la red.

Hay virus que sustraen documentos de los ordenadores que infectan, o que buscan determinados tipos de archivos y los destruyen o que distribuyen archivos personales a terceros al azar.

Como es dable apreciar, la problemática de los virus no solo alcanza al bien jurídico patrimonio –por el daño a la información– sino también a otros bienes jurídicos como los secretos comerciales e industriales, la seguridad de las empresas y de individuos y hasta la privacidad de los datos personales de terceros.

Los virus hoy día se han expandido a todos los ámbitos de la informática y las telecomunicaciones funcionando en las mas diversas plataformas y sistemas. Es posible encontrarlos infectando los programas macro en procesadores de texto y planillas de cálculo, en las redes de distribución y servicios de intercambio de archivos (tales como KaZaA, Bit Torrent u otras basadas en tecnología *peer to peer*), canales de chat (IRC), las redes de teléfonos celulares digitales (smartphones), los sistemas de mensajería instantánea, y constantemente siguen apareciendo "worms" y spyware que instalan programas y rutinas en forma subrepticia con otra finalidad, generalmente de publicidad, y que suelen equipararse a los virus. Los programas se infiltran a través de páginas web, de bugs en los programas de clientes de correo o en los servidores de Internet, y producen las mas variados resultados con sus rutinas de daños.

Todo este fenómeno no podía pasar desapercibido para el derecho penal. Tanto en Argentina como en el extranjero se formularon denuncias que obligaron a los tribunales a pronunciarse sobre estos hechos. En algunos países también se aprobaron leyes especiales para contemplar estas nuevas modalidades delictivas.

2. Aplicación del Código Penal argentino a los virus informáticos.

En nuestro país no se había planteado judicialmente hasta el año 2001 si el accionar de un virus podía ser calificado como delito.

6 Palazzi, Pablo, Delitos informáticos a través de Internet en la República Argentina, Revista Brasileira de Ciências Criminais, ano 11, no. 44 -julho- setembro 2003, pag. 63.

En el año 1993, un tribunal tuvo que decidir si el borrado manual por una persona de datos almacenados en un disco rígido podía encuadrar dentro del delito de daño, efecto que es el que generalmente buscan o producen los virus. Si la respuesta es afirmativa, gran parte del accionar de los virus informáticos quedaría cubierta por esta interpretación. A partir del año 2001 los casos de virus y daño informático fueron mucho mas frecuentes.

2.1. Caso Pinamonti

En el caso "Pinamonti"[7], la Cámara del Crimen de la Capital sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño (art. 183 del Código Penal[8]), pues el concepto de cosa es aplicable al soporte y no a su contenido.

2.2. Caso Vecchio

El tribunal describió el hecho de la siguiente forma "conforme se desprende del auto impugnado el hecho que se investiga en estas actuaciones habría tenido lugar el 26/4/1999, aproximadamente a las 11:00 hs., oportunidad en la cual 103 sucursales del Banco Río dejaron de operar en línea, al tiempo que en la pantalla apareció un mensaje que decía "hasta la vista baby", siendo que a partir de ese momento todas las terminales operativas dejaron de funcionar. Se determinó que dicha falla obedecía a una orden emanada de la computadora asignada a .... (dirección I.P. 172.18.222.165), quien juntamente con los restantes imputados en autos se desempeña como empleado de CEI Tech S.A., realizando tareas de soporte técnico para el producto Home Banking, que comercializa la citada entidad bancaria...".

En primera instancia se procesó al imputado por el delito de daño, resolución que fue apelada por la defensa. La cámara confirmó esta decisión. Para ello se sostuvo que configura el delito de daño la inserción dolosa de un programa destructor en un sistema en red, con la afectación de todas las terminales, ya que no se requieren especiales conocimientos técnicos para la realización de dicha conducta[9] . Es impor-

7 C. Nac. Crim. y Corr., sala 6ª, 30/4/1993, - Pinamonti, Orlando - JA 1995-III-236 y nuestro comentario al fallo publicado en el mismo lugar. El mismo criterio se repite en C. Nac. Crim. y Corr., sala 6ª, 30/08/2001 - "CÚNEO LIBARONA, Rafael", donde se investigaba la sustracción de datos informáticos de una base de datos.-

8 Esta norma dispone "183. Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, 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".

9 C. Nac. Crim. y Corr., sala 1ª, 20/7/2001 - Vecchio, Pablo A., documento Lexis N° 60002183.

tante destacar que la persona que insertó el virus fue filmada por las cámaras del banco, existiendo por ende registro en la filmación y en los "logs" de conexión de la introducción del virus con fecha en ambos casos. El imputado había reconocido ser la persona que estaba en el video lo que la Cámara tuvo en cuenta para confirmar el procesamiento.

El juez de instrucción sobreseyó a los imputados del delito previsto en el art. 72 de la ley 11.723[10] (reproducción ilícita de software) y en atención a las penas se declaró incompetente y remitió las actuaciones al fuero correccional. En esa instancia la querella solicitó la realización del juicio y el magistrado correccional dictó un fallo muy extenso y completo en el cual concluyó que la conducta investigada no constituía delito penal[11].

En el citado fallo se reconoce que la energía eléctrica puede ser objeto de delitos contra la propiedad, como el hurto y robo, lo que en alguna medida implicó reconocerle —al menos a los efectos penales— las calidades de la cosa.

Luego se recuerda que la "información" contenida en un programa o "documento informático" puede ser medida y evaluada, además de que dicho campo magnético se aloja en el soporte que efectivamente es un objeto material, con lo que constituye una característica más de por qué podríamos asimilar la "información" a las disposiciones referentes a las cosas. Y se agrega que el delito de daño no es aplicable al borrado de información, en razón de que no se encuentra expresamente tipificado en nuestro Código Penal, resultando en consecuencia necesaria una modificación o la aprobación de los proyectos de ley oportunamente presentados ante el Poder Legislativo que así lo permitan porque de lo contrario se vulnerarían disposiciones de raigambre constitucional (art. 18 C.N.).

Tal conclusión se funda en un argumento legislativo: el legislador puedo haber modificado la ley y no lo hizo. En concreto el fallo dice que: "...aun cuando en la especie se considerasen reunidos los verbos típicos establecidos en el Código Penal

10 Esta norma dispone que "Sin perjuicio de la disposición general del artículo precedente se considerarán casos especiales de defraudación y sufrirán la pena que él establece, además del secuestro de la edición ilícita:

a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabiente;

b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto;

c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto;

d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados".

11 Juzg. Corr., n. 9, Secretaría n. 65, 14/4/2004 - Vecchio, Pablo A., sentencia de la Dra. Ana Díaz Cano, publ. en Revista Derecho y Nuevas Tecnologías Nos. 6/7, Ad Hoc, 2006.

para el delito de daño, y la ajenidad del objeto (por decirlo de algún modo), lo cierto es que éste debe tratarse de una cosa, no cualquiera, sino una mueble o inmueble, o un animal, o las que por ley le son equiparables, datos éstos que no se corresponden con un ente inmaterial como es el dato informático, por más que se insista en su valor y su factible apreciación, porque es la misma ley quien dejó de lado la cuestión, pese a que tuvo la oportunidad de modificar la norma para delimitar y describir conductas como la aquí analizada".

En concreto se concluye que "...fue el mismo ordenamiento legal (art. 2311, según el texto de la ley 17711) quien vino aunque sólo a equiparar las disposiciones referentes a las cosas, a la energía y a las fuerzas naturales, mas no a darles a éstas esa calidad de cosa, ello así, siempre que sean susceptibles de apropiación, pero nótese que el legislador penal, aun cuando conocedor de la existencia de la problemática de la informática y de los perjuicios que conductas como la investigada podrían ocasionar, optó por proteger otros bienes jurídicos a través de la creación de las correspondientes normas, soslayando ampliar el tipo penal correspondiente al daño, cuando, a juzgar por los antecedentes jurisprudenciales que se han citado en la materia, ya se conocían los efectos que se producían desde esta óptica, e incluso existen proyectos legislativos en tal sentido, motivo por el cual no es posible argumentar, como lo hicieron aquellos antiguos juristas respecto de la energía eléctrica, que el legislador quedó atrasado frente a la tecnología de avance, por cuanto cuando dictó aquellas normas penales basadas en la cuestión informática el "daño informático" era un dato de la realidad por todos conocido".

2.3. Caso Gornstein

El 26 de enero de 1998 la página web de la Corte Suprema de Justicia de la Nación (www.csjn.gov.ar) amaneció con un presentación diferente a la usual. Un grupo de hackers se había infiltrado en el servidor de la misma y reemplazó la página original por una página alusiva al asesinato del periodista José Luis Cabezas. A raíz de ello se iniciaron actuaciones penales que permitieron determinar los autores del acceso y borrado de la página web de la Corte Suprema. También fue muy amplia la prueba recolectada en el sumario. Como bien señala Riquert, mas que un caso de acceso ilegítimo o "hacking" éste era un caso de daño, pese a que el primer tramo de la conducta consistió en un acceso sin permiso[12].

Se debía determinar si constituye delito de daño el ingreso no autorizado y borrado de la página web de la Corte Suprema de Justicia de la Nación. El fallo del Juzgado

12 RIQUERT, M.A. Delitos Informáticos, pag. 322 en Derecho Penal de los Negocios (Carrera, Daniel y Vázquez, H., directores), Astrea, 2005

Nacional en lo Criminal y Correccional Federal Nº 12, en el caso "Gornstein"[13] dio una respuesta negativa. Para así decidir, el juez sostuvo que la página web no era un objeto corpóreo, y por ende no estaba comprendida dentro del concepto de cosa del art. 2311 del Código Civil. Para el juez, una interpretación contraria implicaría lesionar el principio de legalidad establecido en el art. 18 CN. Finalmente se cita el proyecto de ley de delitos informáticos en trámite ante el congreso —que contempla la figura del daño informático— como ejemplo de la necesidad del cambio legislativo advertida también por el legislador.

El fallo no fue apelado, y por ende quedó firme. La Corte Suprema, ante el resultado, solicitó a la Procuración General de la Nación que formara una comisión para elaborar un proyecto de ley.

2.4. Caso Debandi

En este caso se atribuyó a los imputados haber efectuado una maniobra ardidosa con la finalidad de causar perjuicio a la firma Fibertel, que se encarga de brindar acceso a Internet, así como también prestar servicios de diseños de páginas web y hosting, procediendo los nombrados al borrado de parte de los datos informáticos que constaban en la página web de la empresa Torneos y Competencias, Dynamo y Cablevisión, mediante la ejecución y descarga de los archivos "b1.asp" y "b2.asp", para posteriormente presentarse como expertos técnicos para resolver la situación por ellos mismos causada, resultando que por los servicios prestados para la reparación del sitio, recupero de información y servicios de programación, habrían ocasionado a la empresa citada un desembolso de unos $ 5.000.

El peritaje informático incorporado al sumario y el allanamiento permitieron comprobar que en los domicilios vinculados a los imputados había computadoras en las cuales se detectó la existencia del virus que podría haber provocado el daño en las páginas web de la empresa querellante. A ello se sumó que estas personas —según explica el fallo—, se habían desempeñado con anterioridad como empleados de la empresa querellante, precisamente en la organización de la programación del sitio web de la empresa Torneos y Competencias.

La mayoría del tribunal sostuvo que si es factible presumir con cierta probabilidad que los daños ocasionados —introducción de "virus" que podría haber provocado el borrado de parte de los datos informáticos que constaban en las páginas web de la empresa querellante— habrían sido solamente el medio propicio para, posteriormente,

13 Juzgado Nacional en lo Criminal y Correccional Federal N° 12, 20/3/2002, Gornstein, Marcelo Hernán, ED 198-506, con comentario de Miguel Angel EMERY, Delitos Informáticos, ED 198-514 y de Jorge Luciano GORINI, La necesaria protección jurídico-penal de la información, ED 198-518.

ofrecer los servicios de reparación del sitio, recupero de información y servicios de programación, lo que habría ocasionado a la empresa citada un desembolso de dinero, procede revocar la falta de mérito[14].

En cambio en su voto en disidencia, el Dr. Donna sostuvo que si no se había probado la relación causal como para atribuir a los imputados el hecho que se les atribuye, corresponde confirmar la resolución que dispuso la falta de mérito.

Como es dable apreciar, se trata de un caso donde el daño informático desempeñó el papel de medio para obtener una suma de dinero, pero no tiene la suficiente entidad para ser el ardid de una estafa. Queda evidente que es una especie de daño agravado por el ánimo de lucro, aunque tal agravante no está contemplado en nuestra legislación.

2.5. Caso Kohler Antelo

Se atribuyó al imputado haber ingresado al portal de Internet de una empresa en forma ilegal y, una vez en su interior, haber borrado, sustraído, modificado y dañado información científica de la página web.

La sala 6° de la Cámara del Crimen[15] —la misma que intervino en el caso "Pinamonti" antes citado— sostuvo lo siguiente: "toda vez que a partir del dictado de la ley 25.036 los programas de computación —su fuente y objeto— y la compilación de datos y otros materiales resultan bienes jurídicos penalmente protegidos, y el art. 2323 CCiv. al efectuar una enunciación de los bienes muebles hace referencia a las "colecciones científicas", la información en soporte magnético debe ser considerada "cosa" a los fines del art. 183 CP". Por tanto, el tribunal entendió que debía revocarse el sobreseimiento decretado.

2.6. Caso Marchione

En el caso "Marchione" la Sala 2° de la Cámara Federal de la Capital Federal procesó al imputado en orden al delito de daño calificado en concurso ideal con interrupción del servicio de comunicaciones, como consecuencia, del envío masivo de emails con virus informáticos[16]. El caso, sin embargo, tuvo sus vueltas que relataremos seguidamente.

14 C. Nac. Crim. y Corr., sala 1ª, 9/8/2002 - Debandi, Natalia, pub. en Bol. Int. de Jurisp. n. 3/2002, p. 252.

15 C. Nac. Crim. y Corr., sala 6ª, 24/11/2003 - Kohler Antelo, Patricio, Boletín de Jurisprudencia n. 36.

16 Cámara Criminal y Correccional Federal, Sala II - Causa n° 22.600, 15/11/2005, "Marchione, Gabriel Gustavo".

El caso se inicia con la denuncia efectuada en febrero de 2001 por la empresa de publicidad Young & Rubicam ante la Policía Federal Argentina contra Gabriel Marchione por la posible infracción a los delitos reprimidos en los artículos 183 y 197 del Código Penal[17].

La empresa se habría visto afectada por un ataque masivo a sus sistemas de informática mediante la introducción ilegítima de decenas de miles de correos electrónicos de diverso contenido acompañados, en la mayoría de las ocasiones, de virus informáticos o programas de destrucción masiva, circunstancia que habría impedido la comunicación normal dentro y fuera de la empresa. Los emails se enviaban falsificando su origen, y haciendo aparecer a empleados y hasta al Presidente de la empresa como los emisores de los mismos. Los empleados de la empresa habrían recibido "spam" con aproximadamente trescientos cincuenta "e-mails" cada uno, siendo los más afectados algunos que habrían recibido más de mil mensajes cada uno, conteniendo insultos y virus informáticos. En otra tanda, el sistema de la empresa experimentó la recepción de dos mil tres, cinco mil ciento veinte y dieciséis mil cuatrocientos correos electrónicos, cuyo tiempo de recepción fue de dos, tres horas con cincuenta minutos y ocho horas, respectivamente.

Un estudio pericial ordenado por el juez de instrucción informó que los daños provocados fueron: la inutilización por varias horas de las cuentas de correo electrónico del personal, del sistema de correo electrónico y de la línea telefónica de la empresa. El mencionado estudio informático señala los efectos que se detallan a continuación:

- Demoras en la entrega y recepción de e-mails de trabajo.
- Caídas en los servidores dedicados al envío y recepción de e-mails y del servicio en sí.
- Corrupción informática en los archivos de procesamiento de los servidores de mail, lo que obliga a tareas de mantenimiento y depuración adicionales en horarios de trabajo.
- Pérdida de e-mails debido a la necesidad de recuperar backups de fechas anteriores por la corrupción mencionada en el punto anterior.
- Interrupciones en los servicios en horarios de trabajo, por tareas de mantenimiento no programadas.
- Tareas de depuración manual de e-mails, usuario por usuario.
- Requerimiento de espacio adicional de almacenamiento de e-mails depurados y en proceso, con el costo aparejado por la compra del hardware necesario.

17 Norma que dispone "197. Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica o telefónica o resistiere violentamente el restablecimiento de la comunicación interrumpida".

- Inutilización por varias horas de la línea telefónica de la empresa Young & Rubicam.

En base al referido informe la juez de instrucción consideró que "el evento investigado se encuentra entre aquellos conocidos como de intrusismo informático (hacking), o aún de destrucción o cambio de información electrónica (cracking), acciones que lamentablemente aún no han encontrado receptación legal en nuestro ordenamiento penal" ... "como así tampoco lo ha acogido la jurisprudencia en la materia, subsistiendo entonces el debate sobre la corporeidad material o funcional que afectan al software, sólo protegido como obra intelectual (ley 25.036 modificatoria de la ley 11.723) impidiéndose así adecuar este tipo de hecho en el tradicional delito de daño contemplado por el artículo 183 de nuestro Código Penal...". Por ello estimó que el hecho se reducía al delito de interrupción o entorpecimiento de las comunicaciones telefónicas previsto en el artículo 197 del Código Penal y, en consecuencia, declaró la incompetencia en razón de la materia.

Por su parte, el magistrado federal a cuyo conocimiento se remitió el proceso en función de la incompetencia decretada, resolvió el 8 de febrero de 2002 que en el caso sólo se configuró un hecho delictivo, cuya tipificación penal recae en el artículo 183 del Código Penal, pues no cabía duda alguna que la conducta del encartado, al enviar correos electrónicos masivos a la empresa, había generado un perjuicio patrimonial real sobre su sistema informático, así como "... que la finalidad del autor del ilícito ha sido la generación de dicho daño, por ende, el accionar debía ser considerado como un fin en sí mismo, necesitado, obviamente de una serie de maniobras imprescindibles (con referencia al artículo 197 del Código Penal) para poder lograr su realización...". En consecuencia responsabilizó al imputado en calidad de autor por el delito de daño, y declaró la incompetencia de la justicia federal[18].

La decisión fue apelada por la querella y la defensa del imputado, y resuelta en definitiva luego de una intervención de la Sala IV de la Cámara Nacional de Casación Penal[19], por la Sala VII de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, a favor del fuero federal.

La Sala VII de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, entendió que "... la desconexión que se alude no hace más que corroborar que la maniobra fue efectiva para privarla de, o al menos entorpecer, ese medio de comunicación, sea cual fuere la línea telefónica desde la cual se pretendiera acceder al administrador de correo y direcciones afectadas". Además, agregó que "... implica descono-

18 Cabe señalar que el mismo magistrado intervino en el año 2002 en el caso antes citado de daño a la página web de la CSJN y allí concluyó, en sentencia firme de primera instancia que no fue apelada por el ministerio público, que el reemplazo del archivo de dicho web site no era delito penal. Ver Juzg. Nac. Crim. y Corr. Fed., n. 12, 20/3/2002 - Gornstein, Marcelo H. y otros s/delito de acción pública, ED 198-506.-

19 C. Nac. Casación Penal, sala 4ª, 19/12/2002- Marchione, Gabriel, JA 2003-II-116.

cer que uno de los objetivos de los autores de esta abusiva actividad informática, como así también la de las más ingenuas pero inútiles cadenas de correos que se reenvían constantemente, es precisamente congestionar a los servidores de correos y las comunicaciones por esta vía. Dejando de lado que la experiencia indica que el ingresar un virus informático en la red de comunicaciones, al introducirse tanto en los correos como en los soportes flexibles y demás instrumentos usuales de tráfico de información electrónica, por la globalidad de la red, perjudica a un número ilimitado de personas y el servicio de comunicación de manera general..." por cuya consecuencia entendió que debía continuar interviniendo el fuero federal[20].

Luego de ello, la Sala I de la Cámara Federal descartó que el hecho investigado pudiera subsumirse en las figuras previstas en los artículos 183 y 197 del Código Penal, o en otra figura penal, por lo que sobreseyó al imputado[21]. Esta decisión fue apelada a la Cámara Nacional de Casación Penal.

En su resolución de fecha 18 de marzo de 2005, la Sala Cuarta de la Cámara Nacional de Casación Penal dictó un importante fallo en el cual exigió un análisis exhaustivo, en función de los hechos descriptos, de los posibles tipos penales en los que pudiera encuadrar la conducta de Marchione, entre los que consignó a los artículos 183, 184 (concretamente aludió a su inciso 5°) y 197 del Código Penal[22].

La decisión de la Sala II de la Cámara Federal que comentamos analiza el encuadre de los hechos bajo dos delitos distintos: a) daño informático e b) interrupción de las comunicaciones, y concluye que el hecho investigado encuadra en ambos. A nuestro juicio, éste es uno de los casos mas importantes en la materia por el profundo análisis de las cuestiones que allí se plantearon.

a) Daño informático

El tribunal consideró que alterar o destruir datos o información grabados magnéticamente en el soporte físico de una computadora configura el delito de daño —art. 183 del Código Penal—, en los casos en que este último no ha sido destruido "físicamente".

El tribunal aclara que un sistema informático se compone del hardware y el software o programa de ordenador. Este último es el componente lógico o "intangible" del sistema informático. El procedimiento realizado por el imputado consistió en alterar ese conjunto de instrucciones, logrando que el hardware ejecute órdenes que se tradujeron en acciones nocivas, no aprobadas por sus legítimos usuarios, siendo el ejemplo más claro el borrado de archivos de datos insertos en el disco rígido. Es decir,

20 C. Nac. Crim. y Corr., sala 7ª, 16/08/2002.

21 C. Fed. Crim. y Corr., sala 1ª, 02/09/2003 - Marchione, JA 2004-III-271.

22 C. Nac. Casación Penal, sala 4ª, 18/03/2005 - Marchione, JA 2005-III-371.

entendió que se produjeron modificaciones perjudiciales "a nivel lógico", razonamiento que resulta compatible con la ausencia de rastros físicos de la maniobra imputada, en el hardware.

La defensa planteó que el software sólo se ve protegido como obra intelectual, y como de la pericia surgía que no se han producido roturas o daños en el hardware no existiría delito de daño. Para el tribunal "la determinación de la existencia del daño, dista mucho de ser una mera cuestión "fáctica"... Por el contrario, se trata de un proceso de valoración que requiere un análisis previo que tenga en cuenta tanto la correcta caracterización del *objeto de acción del delito*, como las diferentes modalidades de la conducta ilícita, relevando especialmente aquella que ataca el funcionamiento de la cosa y no su entidad corpórea....".

El tribunal parte de un criterio sustentado en la realidad de las cosas, y sostiene que la acción delictiva del delito de daño estuvo dirigida hacia el sistema informático en su totalidad —como conjunto "soporte físico-software"—, y no sólo a este último. Ello es así porque a juicio del tribunal "los dos elementos mencionados conforman una unidad compleja "tangible-lógica", donde ambos componentes se requieren mutuamente para que el sistema opere, es decir cumpla con la función predeterminada y esperada por el usuario". Esto lo lleva a concluir que la destrucción del hardware implica la del software y viceversa. Es decir, a criterio del tribunal: "hardware y software (o datos) forman un todo inescindible y la afectación de uno implica la del otro. Agrega finalmente que "...conforme a esta reformulación de un objeto de acción de naturaleza mixta, puede concluirse sin esfuerzo que éste sí reúne los requisitos de cosa en el sentido del art. 2311 del C.C., ya que está compuesto —además de una parte intangible— de una parte claramente material- soporte físico".

De allí concluye que el resultado causado por la conducta imputada en la parte intangible o programa del sistema, se traslada también, de alguna manera, al componente físico de la mentada unidad compleja y agrega que "se afectó al sistema informático en su funcionalidad, lo que se corrobora con la prueba producida en el caso"[23].

El tribunal recuerda que la doctrina nacional al definir la acción típica del delito de daño explica que ésta consiste en todo ataque a la materialidad, utilidad y disponibilidad de las cosas que elimine o disminuya su valor de uso o de cambio agregando que se ataca su utilidad cuando se elimina —o disminuye— su aptitud para el fin o los

23 El tribunal recuerda lo siguiente:"En este contexto deben valorarse los efectos causados por el virus "Vanina" encontrado en los medios magnéticos analizados en el estudio pericial practicado en la causa, donde se los describe como:"...modificación de los registros del sistema de manera que se pierdan los enlaces de los programas con los archivos de uso más común, por ejemplo, a partir de ese punto, ya no se podrá abrir un documento de Word haciendo doble clic en el mismo....tampoco es posible ya navegar por Internet, debido a que queda desconfigurado el Internet Explorer".

fines al que estaba destinada. Concluye al respecto que "Este criterio de utilidad desarrollado por la doctrina para describir una de las modalidades de la acción típica de daño, impone percibir a la alteración o destrucción de instrumentos lógicos, integradamente a su medio —soporte físico— y no en forma aislada, como pretende la defensa, ya que la conducta realizada termina afectando, en definitiva, la función que cumple el soporte, y atacando por ende, la utilidad que se pretende del sistema informático en su totalidad, así como su valor de uso".

En fin, con un criterio sumamente realista, y apoyado en la pericia realizada en el caso finaliza diciendo "En el caso de autos el informe pericial da cuenta de ese trabajo generado por la acción dañosa, al enumerar los efectos que causaron las conexiones denunciadas, destacando, entre otros, la pérdida de mensajes de correo electrónico debido a la necesidad de recuperar copias de seguridad de fechas anteriores por la corrupción informática generada en los archivos de procesamiento de e-mails, caída en los servidores, tareas de depuración manual de correos electrónicos usuario por usuario, señalando que casi todos los puntos mencionados implicaban una carga adicional de horas/hombre de trabajo...".

El fallo interpreta que un "archivo informático" queda comprendido en el tipo penal de daño agravado (art. 184 del C.P.[24]). Ello así por cuanto "el archivo informático mantiene la sustancia del archivo «tradicional», esto es, las características que permiten describirlo como tal, radicando su «novedad» sólo en el soporte donde se encuentra almacenada la información".

b) Interrupción o entorpecimiento de la comunicación telefónica

El tribunal luego analiza el delito de interrupción o entorpecimiento de la comunicación telefónica prevista por el artículo 197 del Código Penal.

24 La norma dispone como agravante de la figura de daño (art. 183 del Código Penal) que "La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutase el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear sustancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos".

El art. 197 CP prohíbe la conducta de interrumpir o entorpecer la comunicación telefónica[25], protegiendo de tal modo a las comunicaciones en sí y no meramente a algunos de los componentes tecnológicos mediante los que ellas se llevan a cabo[26].

El tribunal tuvo en cuenta que del informe realizado por el perito se desprende que durante numerosas jornadas la empresa recibió una enorme cantidad de correos electrónicos bajo la modalidad "spam", utilizándose para ello un programa conocido como "mail bomber", que virtualmente paralizó la actividad de la empresa denunciante durante varias horas. Además, en los medios magnéticos analizados se constató la existencia de mensajes que tenían adjuntos archivos, que contenían programas que generan y transmiten virus informáticos, y los desarrollos de archivos ".bat", virus todos que fueron recibidos por el denunciante. Finalmente se precisa que "con el objeto de estimar el tiempo de ocupación que insumieron las conexiones denunciadas, se efectuaron pruebas en escala de los ataques sufridos, las que determinaron que si se toman en cuenta los 84.039 correos electrónicos recibidos, con un "peso"[27] de 9.096.836 kb la ocupación del servicio informático y la línea telefónica hubiera sido de 1094 horas, lo que equivale a 45 días y 14 horas".

Por ello el tribunal concluyó que como consecuencia de las conexiones denunciadas se vieron suspendidas o demoradas las comunicaciones del correo electrónico en la empresa y que la interrupción de este medio de comunicación alteró uno de los elementos importantes de su mecanismo de producción y perjudicó su operatoria habitual. Además, resultó el medio idóneo para producir el daño calificado. En base a las reflexiones expuestas el tribunal concluye que la maniobra descripta y llevada a cabo por el imputado encuadra legalmente en el tipo penal de daño agravado (art 184, inciso 5to del Código Penal, en función del artículo 183 CP) en concurso ideal con interrupción o entorpecimiento de línea telefónica (artículo 197 CP).

Cabe resaltar que la tipificación como interrupción de comunicaciones se asemeja mucho a un ataque por denegación de servicios. Esta figura todavía no ha sido tipificada en los países mas desarrollados pero es una forma de daño a sitios de Internet y a la posibilidad de comunicación o acceso a los mismos[28].

---

25 El concepto del tribunal es muy amplio. El tipo penal se refiere a "comunicación telegráfica o telefónica" pero hoy en día las comunicaciones a través de Internet por medio de banda ancha —cable módem o servicio ADSL- o redes wi-fi parecen algo muy distinto. Por otra parte cabe preguntarse, frente al fenómeno de la convergencia, cómo encuadrar en estas categorías el uso de telefonía a través de Internet (VoIP). ¿Se trata de una comunicación telefónica tradicional a través de Internet o un nuevo medio de transportar la voz distinto a la telefonía?

26 Se cita C.N.C.P., Sala IV, causa n° 4447, reg. 6452.4 de fecha 18-3-05.

27 En la jerga informática se habla del "peso" de un archivo para referirse a su extensión medida en Kbytes o en Megabytes.

28 Ver ARRECHE, María Karina, Internet y el bloqueo de servicios (o "denial of service attacks"), en Derecho Informático 1, pag. 59, Iuris.

3. Necesidad de tipificar el delito de daño informatico y el de creación o difusión de virus informático

El delito de introducción de virus en una computadora no está contemplado específicamente en nuestro ordenamiento jurídico penal. Sin embargo, como ya hemos expresado y argumentado en otros trabajos[29], entendemos que el delito de daño es aplicable al caso.

La acción consistiría en contaminar una computadora, ya sea a través de una línea telefónica por un módem o insertando directamente un diskette que se sabe infectado. El aspecto subjetivo requiere no sólo el conocimiento del carácter dañino del programa (no se requiere que sea específico: esto es, entender el mecanismo lógico de cómo daña el virus, sino solamente que dañe), sino también el conocimiento y la voluntad de que causará esos efectos en ese ordenador. El dolo podría ser eventual si el autor no sabe cuando se activará el virus, o en que computadora se activará, pero si la destrucción de la información ocurre por mera culpa no existe delito de daño.

La generalidad de la doctrina ha considerado delito la activación de un virus informático[30]. Pese al vacío legislativo mencionado, las acciones que un virus provoque en el mundo real son susceptibles de ser juzgadas por las normas penales cuando afecten bienes jurídicos tradicionales[31].

Sin perjuicio de ello, nosotros propusimos en su momento[32] incluir en el artículo 183 CP el término "intangible" a la lista de elementos pasivos de daño, con lo que quedaría : "Será reprimido con prisión de quince días a un año, el que destruyere,

29 PALAZZI, Pablo, Virus Informáticos y Responsabilidad Penal, LL 1992-E-1122; y Delitos Informáticos, Ad Hoc, 2000, pags. 144 y ss.

30 Véase FERNANDEZ DELPECH, Horacio, Internet: su problemática jurídica, pag. 195/196; PELLICORI, Oscar, "Informática y Delito", El Derecho, diario del 6/6/94; DALL'AGLIO, Edgardo Jorge, "La responsabilidad derivada de la introducción y propagación del virus de las computadoras", ED 135-903; SAEZ CAPEL, Jose, Informática y Delito, Ed. Proa XXI, pag. 134; KUTTEN, L.J., "Virus Informáticos y Responsabilidad" en Derecho de la Alta Tecnología No. 23, pág. 1; PALAZZI, Pablo Andrés, "Virus Informáticos y responsabilidad penal", LL 1992-E-1122; CARO, Rodrigo, El archivo almacenado en soporte informático como objeto de delito de daño, art. 183 del Código Penal, LL 2004-A-1436; FREELAND, Alejandro, Internet y Derecho Penal, JA 2000-II-769 y FORNAGUEIRA, Andrea, Utilización de los virus informáticos: una nueva conducta delictiva, en Semanario Jurídico 1991-A, pag. 4 a 6, entre muchos otros. Sobre los aspectos civiles ver Carlos PARELLADA, Responsabilidad Civil y Hackers en la responsabilidad (homenaje al profesor doctor Isidoro Goldenberg), (Alterini, Atilio A. - López Cabana, Roberto, directores), Abeledo Perrot, Buenos Aires.

31 Así, la hipotética muerte producida a un paciente, al alterar o retrasar un virus el funcionamiento de una maquinaria médica controlada por computadora, podría ser calificada como homicidio culposo, e incluso como homicidio por dolo eventual si el virus fue introducido en las computadoras del hospital teniendo conocimiento del daño que ocasionaría.

32 Ver PALAZZI, Pablo, Delitos Informáticos, pag. 144 y ss.

inutilizare, hiciere desaparecer o de cualquier modo dañaré una cosa mueble o inmueble o un animal o intangible, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

4. Los virus informáticos como protección de la propiedad intelectual y los negocios contractuales

Los virus informáticos pueden ser usados como una herramienta para la protección de los derechos intelectuales y los negocios contractuales. Pero no siempre estas conductas pueden resultar ajustadas a derecho.

Si un programador inserta un virus en un programa a fin que, en caso de copia, el mismo se active y destruya la información existente en el ordenador es posible considerar la situación como un daño informático además de un abuso de derecho (art. 1071 Código Civil). Si bien el titular de la obra de software está en su derecho de proteger sus intereses como autor o dueño, dicha facultad no debe extenderse más allá de lo que razonablemente expliciten las leyes, o el contrato que lo relacione con el usuario.

Así, cabe plantearse la situación de que el sistema de seguridad anti-copia —conocidos generalmente como dispositivos de "self-help"— sólo se limite a borrar o detener el programa dejando intactos los datos del usuario. En tal situación el productor de software no está —a nuestro entender- infringiendo norma de derecho penal alguna para el caso que haya previsto esta facultad en el contrato de licencia, y no haya transferencia de propiedad del software ni de las copias. Si bien la vía correcta en ese caso es demandar judicialmente el secuestro y destrucción de la copia ilegítima, luego de revocar la licencia.

Por último cabe tratar aquí el caso del programador que usa un virus como medio extorsivo para forzar el cobro de sus honorarios. Suele suceder que luego de la confección de un sistema a medida, el programador exige el pago de lo pactado, y ante la reticencia de la empresa se activa un software dentro del propio sistema que detiene el funcionamiento del programa o lo borra, incluyendo el sistema operativo. El cliente queda como rehén del programador.

En estos casos, quien quiera reclamar el cumplimiento a la otra parte de un contrato debe iniciar las acciones legales pertinentes, pues de otra manera se coloca en una posición de incumplimiento que le impide jurídicamente reclamar el cumplimiento a la contraparte (arg. Art. 1204 CC).

En los Estados Unidos el accionar descripto ha sido tipificado en algunos códigos penales como delito, y existen casos de procesos penales por el uso de estos medios por parte de programadores o empresas para forzar el pago de sus acreencias[33]. La

33 BIERCE, Willian, "El Delito de 'violencia tecnológica' en la legislación de Nueva York", en Derecho de la Alta Tecnología No. 66, pág. 20, Febrero 1994 (traducción de Pablo Palazzi y Antonio Millé). Se comenta el caso de un programador que intentó obtener el pago de sus acreencias mediante un programa virus y terminó con un proceso penal en su contra.

doctrina estadounidense critica la posibilidad de permitir estas facultades al autor de un software, incluso para defender su propiedad intelectual, ya sea que se base en la ley[34] o en un derecho proveniente del contrato[35]. Hoy en día la discusión de estos temas ha cambiado radicalmente por la existencia de dispositivos DRM contemplados en el Tratado de Derecho de Autor de la OMPI, que se usan para proteger la propiedad intelectual[36], y por el uso de Internet para "bajar" y activar software, lo que en los hechos da un mayor control al fabricante del programa.

En Italia la ley del 23 de Diciembre de 1993 no. 547/93[37] ha modificado e integrado algunas normas del Código Penal en materia de criminalidad informática. En el art. 392[38] del Código Penal italiano se agregó un nuevo párrafo que establece el delito denominado ejercicio arbitrario de la propia razón con violencia sobre las cosas, pero aplicado a los programas de computación.

5. Responsabilidad civil por la propagacion de un virus informatico

Un caso interesante ocurrido en Francia es el del virus que infectó a un disquete de prueba que se incluía en una revista francesa especializada en informática. Una empresa adquirente de la revista demandó a la sociedad editora y el tribunal responsabilizó a la demandada por los daños ocasionados por el virus incluido en

34 Ver Raymond T. NIMMER, The Law of Computer Technology, 7.33, pag 111 (2d ed. 1992); Henry GITTER, Self-Help Remedies for Software Vendors, 9 Santa Clara Computer & High Tech. L.J. 413 (1993); Stephen L. POE y Teresa L. CONOVER, Pulling the Plug: The Use and Legality of Technology-Based Remedies by Vendors in Software Contracts, 56 Alb. L. Rev. 609 (1993); Lance A. Raphael, Note, Teaching an Old Law a New Trick: Repossessing Software Through Disablement, 97 Com. L. League of Am. 276 (1992).

35 Esther C. Roditti, Is Self-Help a Lawful Contractual Remedy?, 21 Rutgers Computer & Tech. L.J. 431 (1995), con detalle de los casos ocurridos en Estados Unidos.

36 El caso extremo es el CD rootkit de Sony BMG que incluyó en sus discos de música y que al intentar escucharlos en una PC la contaminaban para evitar la copia de los archivos musicales. La opinión pública fue tan fuerte que Sony se vio obligada en los Estados Unidos y en Canadá a retirar todos los discos con el sistema XCP de protección del mercado. Pero se calcula que cerca de medio millón de ordenadores aun poseen el software insertado subrepticiamente por Sony. Estas actividades, a mi juicio, rozan el acceso ilegítimo y el daño informático. Ver para mas información http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy

37 Gaceta Oficial No. 305, del 30 diciembre de 1993.

38 El artículo 392 del Código penal italiano dice "Esercizio arbitrario delle proprie ragioni con violenza sulle cose. Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giuduce, si fa arbitrariamente ragione da se' medesimo, mediante violenza sulle cose, e' punito a querela della persona offesa, con la multa fino a lire un milione. Si ha, altresi', violenza sulle cose allorche' un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico".

el disquete a titulo de garantía por vicios ocultos en aplicación del art. 1641 del código civil francés[39].

En la apelación se alegó que el virus constituía el hecho de un tercero que presentaba las características de imprevisible e irresistible por lo cual la sociedad demandada no debía responder.

La Corte de casación[40] rechazó esta argumentación sobre la base que el fallo había sostenido que el riesgo de contaminación por virus era un riesgo conocido en el ambiente informático. Para así decidir se basaron en i) la abundante literatura existente en torno a la detección y supresión de virus informáticos, ii) que la sociedad demandada había también elaborado un programa antivirus, lo que confirmaba su pericia en este campo y su calidad profesional y iii) que había procedido a controlar el disquete incluido en la revista, demostrando que el control era usual y posible de realizar. Este fallo tiene importancia como veremos, por el nivel de diligencia y responsabilidad que cabe exigir a un profesional informático y a las empresas que manejan información, lo que en parte implica estar amparado por un programa antivirus suficientemente actualizado.

Sin embargo la postura que aplica los vicios redhibitorios al software no resulta mayoritaria en ese país. Al respecto André Bertrand sostiene que a causa de su naturaleza particular, los conceptos de garantía y vicios ocultos (art. 1641 del CC francés) no son aplicables al software de la misma manera que al equipo informático. Y señala que la jurisprudencia admite que los programas de computación pueden estar afectados por errores, y tanto las costumbres como los contratos los distinguen en función de su naturaleza y de sus defectos[41].

6. Legislación sobre daño informatico y virus en el derecho comparado.

6.1. Evolución del concepto de la propiedad informática bajo el "common law"

Puede decirse que en general, frente al desarrollo de la informática y su aplicación en todas las industrias, el common law evolucionó en su concepto de propiedad[42].

---

39 Revue Trimestrelle de Droit Civil, No. 2 (avr.-jun. 1998).

40 Com. 25 nov. 1997, Société Excelsior Informatique et autre c/ Societe Agi 32, Bull. Civ. Iv, n. 318; D.Aff. 1998.66; Contrats, conc. Consum. 1998.comm.43, obs. L. Leveneur. El resultado sería el mismo en los Estados Unidos. Ver al respecto Vicky H. ROBBINS, Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software, 10 Computer Law pag. 20 (1993).

41 BERTRAND, André, DAT en el momento del problema del año 2000, en Derecho de la Alta Tecnología, Septiembre de 1998, No. 121, año XI, pag. 14.

42 Meiring DEVILLIERS, Virus Ex Machina: Res Ipsa Loquitur, 2003 Stan. Tech. L. Rev. 1.

Así se entendió que el daño a la información contenida en una computadora podría tener lugar sin que existiera destrucción física de la cosa, lo que incluía daños producidos por la imposibilidad de uso de un ordenador[43] y virus liberados dentro del mismo[44]. Los casos son numerosos y comentamos seguidamente los fallos no solo penales sino también civiles, que influyeron en una concepción amplia del término propiedad que aplicaron los jueces.

Por ejemplo, un tribunal en Nueva York condenó al imputado por haber manipulado un ordenador de un tercero, instalando una bomba lógica que hizo que el sistema se "cayera" temporariamente[45]. Otro tribunal en el estado de Texas condenó a un individuo por el delito de acceso y daño a un ordenador al haber usado un código informático que afectó la información sobre pagos de salarios de una empresa[46].

En el caso "In re Brandl"[47], el actor demandó al operador de su sistema informático y tenedor de sus libros comerciales, alegando que éste había insertado un virus informático en su sistema operativo. La demanda de carácter civil se fundó en la teoría de la interferencia intencional con relaciones contractuales de terceros, pero como el demandado no contestó la demanda, se emitió un fallo en su contra en rebeldía.

Algo similar ocurrió en Inglaterra. Una serie de casos ingleses había sostenido que la acción de alterar un disco magnético constituía un daño a la propiedad ajena. En el leading case inglés en la materia, el razonamiento fue similar al del caso "Marchione". El juez Lord Lane de la Corte de Apelaciones sostuvo que el interferir con los datos o informaciones almacenados en un disco disminuía su utilidad y por lo tanto constituía un daño a la propiedad amparable penalmente[48]. El tribunal enfatizó el efecto tangible (disco y ordenador no utilizable) que tenía el menoscabo a la propiedad intangible (los datos electrónicos).

Incluso, aunque un virus no destruya o altere la información, se considera que bajo el common law se afecta la propiedad si consume recursos informáticos de un

43 CompuServe v. Cyber Promotions, 962 F.Supp 1015 (S.D. Ohio 1997); Thrifty Tel, Inc. v. Bezenek, 46 Cal.App. 4th 1559 (Cal. Ct.App. 1996). Ver el comentario al primer caso en la nota citada en el punto inmediato anterior.

44 North Tel, Inc. v. Brandl (In re Brandl), 179 B.R. 620 (Bankr. D. Minn. 1995).

45 Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis, 588 N.Y.S.2d 960, 961 (New York City Civ. Ct. 1992).

46 Burleson v. State, 802 S.W.2d 429, 432 (Tex.App. 1991); Ver también los siguientes casos utlizando los mismos conceptos: United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990); Ward v. Superior Court, 3 CLSR 206 (Cal. Super. Ct. 1972); United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

47 North Tel, Inc. v. Brandl (In re Brandl), 179 B.R. 620 (Bankr. D. Minn. 1995).

48 R v. Whiteley 93 Crim.App. R. 25 (Eng. CA 1991).

ordenador[49], por ejemplo a través del envío de correos electrónicos no solicitados, que inundan un servidor ajeno y disminuyen su funcionamiento óptimo o el uso de tiempo de ordenador sin permiso del dueño.

6.2. Legislación y jurisprudencia en Estados Unidos.

El adelanto que Estados Unidos representa en materia de alta tecnología corre a la par de sus leyes. En 1984 se sancionó a nivel federal la "Ley contra el Abuso y Fraude Informático" (Counterfeit Acces Device and Computer Fraud and Abuse). Esta ley fue modificada en repetidas oportunidades para adaptarla a los cambios de la tecnología[50] y el gobierno federal se preocupa constantemente por perseguir penalmente a sus infractores como lo evidencia su sitio de Internet dedicado al "cybercrime"[51].

La citada 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.

Con la finalidad de eliminar discusiones interminables sobre el concepto de virus, gusano (worm), caballo de Troya, etcétera y en que difieren unos de otros, la ley federal prohíbe la transmisión de un programa, información, códigos o comandos que causan daños al ordenador, al sistema informático, a las redes, información, datos o programas[52]. De esa forma, sin definir a estos programas, se los define por su resultado. Como veremos mas adelante, la ley federal fue la primera en ser aplicada a caso de un virus propagado por Internet en forma global, generando luego leyes estaduales específicas[53].

---

49 Meiring DEVILLIERS, Virus Ex Machina: Res Ipsa Loquitur, 2003 Stan. Tech. L. Rev. 1, con cita del caso CompuServe v. Cyber Promotions (962 F.Supp. at 1022) y los casos United States v. Sampson, 6 CLSR. 879 (N.D. Cal. 1978) (se condenó al imputado por apropiarse del tiempo y recursos informáticos propiedad del gobierno). Otros tribunales, sin embargo, se negaron a asimilar a un derecho de propiedad el uso de recursos informáticos: ver Indiana v. McGraw, 480 N.E. 2d 552 (Ind. 1985); New York v. Weg, (NY Crim. Ct. 1982).

50 Ver las normas federales actualizadas en http://www.cybercrime.gov/fedcode.htm

51 Ver http://www.cybercrime.gov/index.html. Por otra parte, el listado de casos, disponible en http://www.cybercrime.gov/cccases.html, demuestra que desde 1998 al 2003 se han obtenido mas de medio centenar de condenas en la materia.

52 Cfr. 18 U.S.C. 1030, que dispone "Section 1030(a)(5)(A)….(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby …. (A) causes loss to one or more others of a value aggregating $ 1,000 or more during any one year period;…".

53 Dentro del delito de daño, algunas leyes estaduales contemplan específicamente a los virus informáticos, como ser California, Illinois, Minesota, Nebraska y Texas. Ver un listado en http://www.ncsl.org/programs/lis/cip/hackleg01.htm

Actualmente la mayoría de los estados poseen una legislación determinada sobre delitos informáticos que de alguna manera, ya sea tipificando la destrucción de información o precisando que constituye delito el uso de virus, ha abordado la cuestión[54].

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.

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.

El caso mas notorio, y primero en que fue aplicada la ley federal fue "United States v.Morris"[55]. En noviembre de 1988, Robert Tappan Morris, estudiante de informática en la Universidad de Cornell e hijo de uno de los mas prestigiosos expertos en seguridad de sistemas informáticos del gobierno (su padre trabajaba para la NSA) introdujo un virus en la red Arpanet. Esta red de computadoras, que actualmente forma parte de Internet, poseía 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. Un error de programación hizo que el virus fuera muy dañino (se replicaba sin cesar hasta agotar los recursos de la computadora infectada).

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 6.000 ordenadores quedaron afectados en sólo tres horas, lo que implicaba 10% de los 60.000 ordenadores entonces existentes en la red[56]. 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

54 Mark R. COLOMBELL, The Legislative Response to the Evolution of Computer Viruses, 8 RICH. J.L. & TECH. 18 (Spring 2002) at http://www.law.richmond.edu/jolt/v8i3/article18.html.

55 928 F.2d 504 (1991). La Corte Suprema no revisó el caso: cert. denied, 112 S. Ct. 72 (1991).

56 Harold Smith Reeves, Property in Cyberspace, 63 U. Chi. L. Rev. 764 (1996).

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 juzgado 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 solo buscó demostrar sus habilidades y lo exponían como baluarte de uno de los campos tecnológicos en el que Estados Unidos mantiene su liderazgo por sobre otros países: la producción de software y de tecnologías informáticas. Morris fue condenado a tres años en suspenso, 10.000 dólares de multa y 400 horas de trabajo comunitario. La Cámara de Apelaciones confirmó esta condena. La doctrina[57] consideró correcta la aplicación que los tribunales hicieron en este caso de la Computer Fraud and Abuse Act de 1986[58].

El tribunal concluyó que para la configuración del tipo penal, bastaba que el imputado intente acceder, y que no resultaba necesario además el acceder y causar daño a un ordenador federal ("federal interest computer"). Basándose en el debate legislativo el Fiscal argumentó que la ley era clara: el Congreso al aprobar la ley previó que el dolo se aplicara sólo al acceso no autorizado y no al daño. Hoy en día esa presunción se podría decir que es superflua. Cualquiera sabe que, con la interconexión existente debido a la red Internet, un virus puede en poco tiempo infectar y afectar a millones de ordenadores. El tribunal condenó a Morris por acceso sin autorización, aunque éste tenía acceso autorizado a los ordenadores de las Universidades de Cornell, Harvard, y Berkeley. Morris también tenía autorización para usar el email y un programa buscador de datos llamado "finger demon," pero se concluyó que no usó estos programas para sus funciones específicas. Finalmente se puntualizó que el virus había sido programado para expandirse a ordenadores en los cuales él no tenía autorización para acceder.

La sentencia en el caso Morris es importante por diversos motivos. La interpretación de lo que es un ordenador de interés federal ("federal interest" computers) es amplísima, pues incluye a cualquier ordenador conectado a Internet. Por ende, cualquier autor de un virus puede ser acusado de acceder sin permiso a estos ordenadores. Además, la interpretación anterior al caso Morris requería que el fiscal probara que el acceso afectaba la operación de un ordenador. Con la doctrina del caso "Morris", solo el acceso intencional y no ya el causar daño intencionalmente es lo punible. Finalmente, también en el caso Morris se concluyó que el uso de una herramienta informática de forma contraria a sus finalidades puede constituir un acceso no autorizado.

57 Ver ente otros Grant E. COFFIELD, Love Hurts: How To Stop The Next "Love Bug" From Taking A Bite Out Of Commerce, en The Journal of Law and Commerce, Spring, 2001, vol 20, pag. 241.

58 18 U.S.C. § 1030(a)(5)(A)-(C) (2000).

Por la época y por la novedad el caso Morris terminó con una condena judicial. Pero actualmente la mayoría de los casos sobre delitos informáticos terminan en "plea agreements", o acuerdos con el Fiscal donde el imputado reconoce su accionar y se le da una pena menor[59].

Sin embargo no han faltado otros casos de condenas por este delito. Por ejemplo en el caso United States v. Sablan[60] se confirmó una condena a una empleada de banco por dañar archivos del servidor central de la entidad una vez que fue despedida. La empleada entró por la puerta trasera y de noche, se conectó al ordenador central y borró numerosos archivos de la entidad financiera.

Mas recientemente, en el caso Hotmail Corp. v. Van$ Money Pie Inc.[61], un tribunal de California sostuvo que el envío de miles de correos electrónicos no solicitados a usuarios de Internet, conteniendo falsas direcciones de origen de los mismos indicando como originante al actor (Hotmail) constituía una violación a las disposiciones civiles de la Computer Fraud and Abuse Act. Esta norma prohíbe transmitir información falsa que cause un daño. Los imputados habían creado direcciones de hotmail.com para recibir allí los pedidos de remoción y los emails que rebotaban por inexistencia de las direcciones de destino y evitar recibirlas en sus cuentas personales. El tribunal entendió que los imputados habían accedido intencionalmente y sin autorización al sistema o servidor de Hotmail al forzarlo a recibir, retener o transmitir a los suscriptores legítimos de esta empresa y desprestigiándolo frente a sus clientes[62].

6.3. Legislación y jurisprudencia inglesa.

En Inglaterra[63] el primer caso de daño informático fue Cox v. Riley[64] resuelto por aplicación de la Criminal Damage Act de 1971 que penaliza a quien sin una excusa legal destruya o dañe cualquier propiedad perteneciente a otro. El imputado Cox utilizaba una sierra computarizada que tenía diversos programas. El imputado utilizó

59 Por ejemplo, el autor del virus Melissa fue condenado a veinte meses en una prisión federal a cambio de su "acuerdo de cooperación" en donde el imputado reconocía haber producido un daño cercano a 80 millones de dólares sólo en los Estados Unidos. Ver http://www.cybercrime.gov/melissa.htm

60 92 F.3d 865, 866 (9th Cir. 1996).

61 Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1998 WL 388389 (N.D. Cal. 1998).

62 Sobre el fenómeno del spam ver PALAZZI, Pablo, Aspectos legales del correo electrónico no solicitado, JA 2004-I-920.

63 Un estudio detallado sobre el daño informático en Inglaterra puede verse en http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim11.html

64 Cox v. Riley [1993] FSR 168 (CA).

uno de los programas para cancelar el funcionamiento de la sierra. Al borrar esos programas, la sierra dejó de funcionar hasta que pudo ser reprogramada. El tribunal entendió como un factor crítico el resultado de la conducta de Cox, pues el propietario de la sierra tuvo que invertir tiempo y dinero en recuperar la sierra a su condición original y por ello fue condenado por el delito de daño[65].

Pero este y otros casos[66] demostraban las limitaciones de las leyes entonces vigentes. Esto generó en el gobierno una comisión de estudio[67] que propuso recomendaciones que dieron lugar finalmente a la sanción de la ley denominada Computer Misuse Act del año 1990, que incluyó la modificación de datos y el borrado de información o programas como delito penal.

Existen varios casos relativos a virus informáticos. En el primero, que ocurrió antes de la reforma de la ley penal, se juzgó a una persona que había sido extraditada desde los Estados Unidos al Reino Unido. Se lo acusó de distribuir cerca de 20.000 disquetes que contenían información sobre el virus del SIDA, y que estaban acompañados de un virus que, luego de cierto uso paralizaba el ordenador y reclamaba al usuario que enviara un cheque a una cuenta de banco en Panamá. Al comienzo del proceso la defensa argumentó la insania del imputado y el caso nunca llegó a juicio.

En junio del año 1992 el imputado que produjo daños por la suma de £ 36,000 a una imprenta en perdidas económicas fue multado con la suma de £ 1,650[68], y en diciembre de 1992 un programador que había implantado una bomba lógica en los ordenadores de su ex empleador causando un daño cercano a los £ 30,000 fue condenado a 140 horas de trabajo comunitario y a pagar una multa de £ 3.000[69].

Esta nueva ley también fue aplicada en noviembre de 1995 en el caso "Pile"[70]. Christopher Pile fue acusado de acceder cinco veces sin autorización a distintos ordenadores y de distribuir dos virus que había escrito ("Pathogen" y "Queeg"). Los virus que Pile difundió a través del BBS causaron cuantiosas pérdidas a empresas británicas. La condena fue de dieciocho meses.

---

65 Mathias KLANG, A Critical Look at the Regulation of Computer Viruses, International Journal of Law and Information Technology, June 2003, vol 11-162, Oxford University Press.

66 R v Whitely, ((1990) y R v Whitely (1991) 93 Cr App Rep 25, CA.) discutiendo si la Criminal Damage Act 1971 podia aplicarse a propiedad intangible.

67 Law Commission's Report No 186, Computer Misuse, (October 1989).

68 Ver "Bedworth case puts law on trial", Computing March 25, 1993, p 7., citado por Andrew Charlesworth ,Addiction and hacking, New Law Journal, Vol 143 No 6596 p 540 (1993), Butterworth & Co (Publishers) Ltd.

69 Ver "Bomber walks free despite Guilty verdict" Computing December 10, 1992 p 3.), citado por Andrew Charlesworth ,Addiction and hacking, New Law Journal, Vol 143 No 6596 p 540 (1993), Butterworth & Co (Publishers) Ltd.

70 R. v. Pile; (1995) unreported.

Sin embargo, pese a todo lo expuesto, un caso reciente fallado en el año 2005 sostuvo que la denegación de servicio no es delito bajo la ley de delito informático del año 1990. En este caso, un adolescente inglés fue absuelto del delito de denegación de servicio que produjo daños al sistema informático de su empleador. Este delito consiste en saturar un servidor con pedidos de acceso o con miles de correos electrónicos a los fines de inutilizarlo temporalmente. En el caso el imputado estaba acusado de haber enviado cinco millones de mensajes de correo electrónico al servidor de la empresa donde trabajaba y de donde había sido previamente despedido[71].

El imputado fue absuelto porque la ley inglesa de delitos informáticos (*Computer Misuse Act of 1990*) no contempla la denegación de servicio como delito. En su momento, hace quince años, cuando Inglaterra reformó sus normas penales para adaptarlas a la informática se legisló el acceso no autorizado y la modificación no autorizada de material informático. La defensa se basó en que el envío de numerosos correos electrónicos no solicitados a un servidor no constituía delito porque el servidor justamente había sido habilitado para recibir correos y bajo la terminología de la ley no se modificaba ni accedía a ningún ordenador.

La decisión del magistrado londinense sostuvo que "el mundo informático ha cambiado considerablemente desde la sanción de la ley en 1990" y agregó que no existían precedentes en la materia. Para absolver al imputado razonó del siguiente modo "En este caso, los correos electrónicos enviados causaron cada uno en forma individual una modificación que fue "autorizada". Aunque fueron enviados en masa, saturando el funcionamiento del servidor, el efecto sobre el servidor no es una modificación punible bajo la sección 3 de la "Computer Misuse Act" concluyendo que ningún tribunal podría concluir en forma razonable que se trataba de e-mails no autorizados.

En este país se estudia desde hace varios años una reforma de la ley para actualizarla al Convenio del Ciberdelito y a las nuevas técnicas delictivas como la del caso comentado, que mediante denegación de servicios anulan termporariamente el funcionamiento de servidores en Internet provocando daños[72] .

6.4. Otros países

Señala González Rus que la proliferación de virus, bombas lógicas y procedimientos similares ha despertado tal preocupación que algunos ordenamientos han previsto

71 Ver la nota de Tom Espiner publicada en http://news.com.com/British+teen+cleared+in+e-mail+bomb+case/2100-7348_3-5928471.html

72 Paul BARTON, publicado en The Lawyer, Junio 28, 2004 y Anne FLANAGAN, The law and computer crime: Reading the Script of Reform, publicado en International Journal of Law and Information Technology, Marzo de 2005, no. 98.

expresamente la difusión de los mismos[73]. Así, el art. 615.5 del Código penal italiano, en el que se castiga con la pena de reclusión de hasta dos años y multa de hasta veinte millones de liras la difusión de programas que tengan por objeto o produzcan el efecto de dañar un sistema informático o telemático, los datos o los programas contenidos en él o pertenecientes al mismo o la interrupción, total o parcial, o la alteración de su funcionamiento[74] .

El artículo 264.2 del Código Penal español castiga con la pena de prisión de uno a tres años al que 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. La doctrina considera que esta norma es aplicable a los virus informáticos[75].

Los españoles optaron por tipificar el daño informático directamente como una figura agravada. Analizando este delito, señala Gonzalez Rus[76] que "la destrucción de sistemas informáticos y de datos, programas y documentos electrónicos es uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito informático. El daño puede afectar tanto a los elementos físicos del sistema (destrucción de un monitor, incendio de una unidad de proceso, inutilización de una impresora, etc.) como a los elementos lógicos. En el primer caso, el tratamiento penal no ofrece particularidad alguna, debiendo aplicarse el tipo básico de daños del art. 263, y eventualmente las agravaciones del art. 264, cuando los daños afecten exclusivamente a objetos físicos del sistema. Cuando los daños alcancen también a elementos lógicos será aplicable, como veremos, la figura agravada del art. 262.2. Los supuestos que resultan más complicados desde el punto de vista penal son, pues, los de destrucción de datos, programas o documentos electrónicos, que son, además, los que han alcanzado mayor notoriedad. Aunque los daños pueden producirse tanto por procedimientos físicos como propiamente informáticos, son éstos los que despiertan mayor interés. La

73 Juan José González Rus, Protección Penal de sistemas, elementos, datos, documentos y programas informáticos, en Revista Electrónica de Ciencia Penal y Criminología, RECPC 01-14 (1999). Este excelente artículo, cuya lectura recomiendo, está disponible en Internet en http://criminet.ugr.es/recpc/recpc_01-14.html

74 BUONOMO, en AAVV, Profili penali dell´informnatica, pag. 82 y ss.

75 Ver Manuel MARCHENA GOMEZ, Prevención de la delincuencia tecnológica, en Derecho de Internet (Rafael Mateu de Ros y Juan Manual Cendoya Mendez de Vigo, coordinadores), Aranzadi Editorial, 2000, Navarra, pag. 439; Juan José GONZÁLEZ RUS, Protección Penal de sistemas, elementos, datos, documentos y programas informáticos, ob. citada; Xavier Ribas, Respnsabilidad por virus, Circular 139, en http://www.onnet.es/07010001.htm; Julio Melón Pérez, Responsabilidad jurídica derivada de la creación y difusión de virus informáticos, en Derecho.com, julio de 2002, http://www.derecho.com/boletin/articulos/articulo0139.htm.-

76 Juan José González Rus, Protección Penal de sistemas, elementos, datos, documentos y programas informáticos, en Revista Electrónica de Ciencia Penal y Criminología, RECPC 01-14 (1999).

proliferación de virus, bombas lógicas y procedimientos similares ha despertado tal preocupación que algunos ordenamientos han previsto expresamente la difusión de los mismos. A esa preocupación responde el art. 264.2, introducido por el Código penal de 1995 y en el que se recoge como modalidad agravada de daños la conducta de 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» (prisión de uno a tres años y multa de doce a veinticuatro meses)".

La inclusión de esta norma en el derecho penal español tuvo su debate. El citado autor explica además que "Aunque ya en el Código anterior nada se oponía a la aplicación del delito a este tipo de elementos, con esta previsión el Código zanja la polémica en torno a la aplicación de los daños a los datos y elementos informáticos, negada para el Código anterior por la doctrina mayoritaria[77]. Ello suponía expulsar del delito a ficheros, programas y aplicaciones y elementos lógicos de redes, soportes o sistemas informáticos, de gran valor económico y que, en cuanto impulsos electromagnéticos, son —de acuerdo con el sentido tradicional de la "corporalidad"— incorporales, aunque tienen un valor autónomo e independiente del que corresponde al soporte magnético en el que se graban. Lo cierto es que los datos son entidades físicas y, en ese sentido, materiales, aunque no sean en sí aprehensibles ni perceptibles de manera inmediata por los sentidos. Sin embargo, sí pueden ser directamente dañados, y por ello objeto material del delito de daños, condición que corresponde a la cosa corporal o incorporal, mueble o inmueble, económicamente valorable, susceptible de deterioro o destrucción y de ejercicio de la propiedad. En todo caso, la previsión expresa resulta oportuna, en la medida en que resuelve las dudas que, por más que resultaran infundadas, pudieran mantenerse al respecto. Que la conducta se conciba como modalidad agravada de daños evidencia, además, que se les da más importancia que a los propios elementos físicos del sistema informático, cuya afectación daría lugar al tipo básico del art. 263".

En Francia resultan de aplicación los arts. 323-2[78] y 323-3[79] del Código Penal, que penalizan el afectar el funcionamiento de un sistema informático o la introduc-

77 El citado autor aclara que el rechazo se basaba en una mala comprensión del requisito de la "corporalidad" o "materialidad" que se exigía al objeto material del delito de daños. Cfr. GONZÁLEZ RUS,Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos, en RFDUCM, Monográfico n.º 12, 1982, pp.107 y ss.

78 Que dice asi "Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende".

79 Que dice "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende".

ción fraudulenta de datos en un programa de ordenador. Estos tipos penales se aplicaron en el mismo caso que comentamos mas arriba (ver punto 5) pero en el proceso penal ocasionado luego del juicio civil contra la empresa que había distribuido los virus[80]. A través del art. 323-3 del Código Penal la jurisprudencia ha considerado bajo esta norma la introducción en un sistema de virus, de programas no autorizados y también se ha aplicado al acceso fraudulento a sistemas informáticos[81].

A través de la ley 19.223, Chile tipificó figuras penales relativas a la informática, convirtiéndose en el único país de la región que ha actualizado su código penal contemplando delitos informáticos. El art. 1° contempla destrucción o inutilización de un sistema informático y la figura de obstaculizar o modificar su funcionamiento. El art. 3 de la referida ley tipifica como delito la acción de alterar, dañar o destruir datos. La ley prevé un agravamiento de pena cuando el autor este a cargo de la red o del centro de cómputos. Ambos delitos son aplicables al caso de los virus informáticos. Según la doctrina, el bien jurídico protegido por esta norma es la integridad de la información en si misma[82].

En Perú el artículo 207º-B dispone que "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa"[83].

En Costa Rica, el artículo 229 bis del Código Penal introdujo la alteración de datos y sabotaje informático. La norma dispone que "Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio acceda, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años".

Finalmente, en Uruguay se interpreta que el art. 358 del Código Penal uruguayo plantea un problema para la tipificación de los virus informáticos por el hecho de

80 Cass. crim., 12 déc. 1996 ; Proc. gén. près CA Paris et a. : Juris-Data no. 005348, JCP G 1997, IV 779. El caso está publicado en internet en http://lexinter.net/JPTXT2/introduction_d'un_virus.htm

81 André LUCAS et al, Droit de l´informatique et de l´internet, PUF Droit, pag. 687.

82 Juan Pablo HERMOSILLA y Rodrigo ALDONEY, Delitos Informáticos, pag. 428, en Derecho y Tecnologías de la Información, Universidad Diego Portales, 2002, Chile.

83 Reforma por ley 27.309 que incorpora al Código Penal del Perú los Delitos Informáticos (Promulgada el 15 de Julio del año 2000).-

que su objeto ha de ser solo una cosa mueble o inmueble y se considera que los datos no se encuentran dentro de esta categorización[84].

Es del caso señalar que la ley de derecho de autor de México ampara los programas de ordenador como obras intelectuales, pero contiene una salvedad en relación al tema que estudiamos que demuestra la opinión negativa que el legislador mexicano tiene sobre los virus informáticos. El Artículo 102 de la citada ley dice "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 la Convención del Ciberdelito[85] dispone en su artículo 4° que "cada parte adoptará las medidas legislativas y de otra especie que sean necesarias para establecer como delito bajo su ley local, a los actos que en forma intencional e ilegal dañen, borren, deterioren, alteren o supriman datos de ordenadores". El art. 1° define el término datos de ordenadores como "cualquier representación de hechos, información o conceptos en una forma tal que permita su procesamiento por un ordenador, incluido un programa que permite que un ordenador realice una determinada función".

La importancia de la Convención se puede apreciar con un caso concreto: el virus conocido como "Love Bug" (o I Love You). Este virus fue elaborado en Filipinas y se expandió rápidamente por todo el mundo[86]. Partiendo de información provista por un ISP en Filipinas, el FBI logró determinar el autor del programa que resultó ser Onel de Guzman, un ex estudiante filipino de ciencias informáticas[87]. Se allanó su casa y se encontraron pruebas de la autoría del virus. Pero había un problema: Filipi-

84 Enrique MULER MENDEZ y Ana BRIAN NOUGRERES, Responsabilidad penal en materia informática en Uruguay, en Derecho Informático, tomo V, pag. 145, FCU, Montevideo, 2004.

85 Convention on Cybercrime (ETS No. : 185), firmado en Budapest, el 23 de noviembre de 2001 por los países miembros del Consejo de Europa. Texto disponible en http://conventions.coe.int/ (traducción del autor). Sobre esta convención ver TILLI, Nicolás, La Convención Europea sobre la "Cyber-criminalidad", JA 2004-I-1241.

86 El virus llegaba a la computadora de la víctima con el mensaje I love You, buscaba en el disco rígido los archivos mp3 y .jpg. Una vez que los encontraba los destruía y los reemplazaba con una copia del virus. Luego redireccionaba el Explorer a un sitio especial donde una nueva rutina escaneaba la computadora de la víctima buscando passwords, log-ins y claves de acceso. Finalmente el virus enviaba una copia de si mismo a todos los nombres de la libreta de direcciones de correo del Outlook.

87 El estudiante fue descubierto porque había presentado una tesis donde desarrollaba un programa espía para robar claves de acceso. Sus profesores consideraron poco ética la propuesta. Con la difusión del virus, relacionarnos los daños con la tesis doctoral y lo informaron a las autoridades.

nas no tenía ley de delitos informáticos, por ende ni el hacking, ni el daño informático ni la distribución de virus o la sustracciones de claves era considerado delito en ese país. Tampoco se lo podía extraditar a otros países donde el virus había provocado innumerables daños y pérdidas pues en todos ellos estaba vigente el requisito de "doble criminalidad", esto es que la conducta sea delito tanto en el país requirente como el requerido. Ante la presión mundial, Filipinas aprobó en cuestión de semanas una ley de comercio electrónico y de delitos informáticos que contemplaba todas las conductas que Onel de Guzman[88] había realizado. Pero la irretroactividad de la ley penal impidió todo castigo. De haber tenido Filipinas una ley de delitos informáticos, o de haber adoptado los criterios previstos en la Convención de Budapest, los daños ocasionados por el virus "Love Bug" no habrían quedado impunes.

7. Conclusiones

Los casos que hemos comentado en esta nota demuestran que una cuestión que parece moderna (los virus informáticos) pero que ya lleva mas de dos décadas de debate aun no ha recibido una respuesta legislativa adecuada en nuestro medio. Mientras tanto, los virus siguen haciendo estragos en las herramientas que a diario usamos para trabajar.

En el último lustro se dictaron una serie de fallos en nuestro país que tratan el problema penal de los virus, con diversos resultados. Las conclusiones inmediatas que surgen de estos casos es que estos delitos informáticos se siguen cometiendo a diario y producen cuantiosas pérdidas a empresas, a individuos y al Estado. Por otra parte, la falta de una legislación especial deja un vacío en una materia que es muy importante amparar.

Existen distintos niveles de daño que un virus o el accionar humano pueden causar a un ordenador. Desde el mas claro que es la destrucción del hardware, hasta el mas sutil borrado de los programas o los datos contenidos en el mismo. En el medio hay diferentes variantes, como la desconfiguración de los programas o periféricos, el encriptado de datos, la alteración de los puertos de entrada o salir del ordenador, los daños aleatorios, o el bloqueo de periféricos o la saturación de servidores mediante miles de pedidos de acceso falsos. Los virus pueden provocar otros daños no relacionados directamente al derecho de propiedad. Por ejemplo, algunos virus toman un archivo al azar y lo distribuyen aleatoriamente a una lista de distribución de correos, pudiendo de esa forma violar la intimidad, el secreto profesional o el secreto industrial. Otros reenvían a la lista de correo del usuario insultos o pornografía, compro-

88 El art. 33 de la ley 8972/2000 contemplaba como delito el daño informático con una pena de seis meses a tres años.

metiendo su honor o identidad. También los ataques coordinados de denegación de servicios en Internet constituyen un grave atentado a la estabilidad de las comunicaciones, que hoy en día son tan indispensables como necesarias para cualquier tarea.

La doctrina —como vimos— es unánime sobre la necesidad de legislar pero también se aclara que ciertas conductas pueden ser delito sin ley especial (el caso del virus que daña el BIOS)[89]. De todas maneras, y mas allá del resultado de los casos que examinamos, parece claro que en Argentina necesitamos con urgencia una ley que modifique el código penal tipificando el daño informático como delito, cuestión que también se ha planteado en el derecho comparado[90] pese a que esos países cuentan con precedentes importantes en la materia[91]. Por otra parte la importancia de estos asuntos puede verse claramente en los efectos que tuvo el virus "Love bug" a nivel mundial que llevó a tomar conciencia de la importancia de la Convención contra el ciberdelito y la necesidad de enfrentar el tema a nivel global[92].

Bibliografía

ARRECHE, María Karina, Internet y el bloqueo de servicios (o "denial of service attacks"), en Derecho Informático 1, Iuris.

BERTRAND, André, DAT en el momento del problema del año 2000, en Derecho de la Alta Tecnología, Septiembre de 1998, No. 121, año XI.

BIERCE, Willian, "El Delito de 'violencia tecnológica' en la legislación de Nueva York", en Derecho de la Alta Tecnología No. 66, pág. 20, Febrero 1994 (traducción de Pablo Palazzi y Antonio Millé).

CARO, Rodrigo, El archivo almacenado en soporte informático como objeto de delito de daño, art. 183 del Código Penal, LL 2004-A-1436.

Kelly CESARE, Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, 14 Transnat'l Lawyer 135 (2001).

89 Leonardo BROND y Sebastián BRIGNANI, Delitos informáticos: panorama deslindante y criterio de demarcación, LL 2004-C-1250.

90 Kelly CESARE, Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, 14 Transnat'l Lawyer 135 (2001).

91 Ver por ejemplo United States v. Sablan, 92 F.3d 865, 866 (9th Cir. 1996) -confirma condena a empleado de banco por dañar archivos del servidor central de la entidad una vez que fue despedido- y United States v. Morris, 928 F.2d 504 (2d Cir.), cert. denied, 112 S. Ct. 72 (1991) —virus que infectó 6000 ordenadores a través de internet-.

92 Shannon C. Sprinkel, The residual effects of the "Iloveyou" computer virus and the draft convention on cyber-crime, 25 Suffolk Transnat'l L. Rev. 491 (2002).

Mark R. COLOMBELL, The Legislative Response to the Evolution of Computer Viruses, 8 RICH. J.L. & TECH. 18 (Spring 2002), http://www.law.richmond.edu/jolt/v8i3/article18.html

DALL'AGLIO, Edgardo Jorge, "La responsabilidad derivada de la introducción y propagación del virus de las computadoras", ED 135-903

FERNANDEZ DELPECH, Horacio, Internet: su problemática jurídica, Lexis 2005.

FORNAGUEIRA, Andrea, Utilización de los virus informáticos: una nueva conducta delictiva, en Semanario Jurídico 1991-A-4.

Anne FLANAGAN, The law and computer crime: Reading the Script of Reform, publicado en International Journal of Law and Information Technology, Marzo de 2005, no. 98.

Henry GITTER, Self-Help Remedies for Software Vendors, 9 Santa Clara Computer & High Tech. L.J. 413 (1993).

Juan José GONZÁLEZ RUS, Protección Penal de sistemas, elementos, datos, documentos y programas informáticos, en Revista Electrónica de Ciencia Penal y Criminología, RECPC 01-14 (1999).

Jorge Luciano GORINI, La necesaria protección jurídico-penal de la información, ED 198-518.

Juan Pablo HERMOSILLA y Rodrigo ALDONEY, Delitos Informáticos, en Derecho y Tecnologías de la Información, Universidad Diego Portales, 2002, Chile.

KUTTEN, L.J., "Virus Informáticos y Responsabilidad" en Derecho de la Alta Tecnología No. 23.

André LUCAS et al, Droit de l´informatique et de l´internet, PUF Droit

Raymond T. NIMMER, The Law of Computer Technology.

Enrique MULER MENDEZ y Ana BRIAN NOUGRERES, Responsabilidad penal en materia informática en Uruguay, en Derecho Informático, tomo V, FCU, Montevideo, 2004.

PALAZZI, Pablo, Delitos informáticos a través de Internet en la República Argentina, Revista Brasileira de Ciências Criminais, ano 11, no. 44 -julho- setembro 2003, pag. 63.

- Virus Informáticos y Responsabilidad Penal, LL 1992-E-1122.

- Delitos Informáticos, Ad Hoc, 2000, pags. 144 y ss.

- Aspectos legales del correo electrónico no solicitado, JA 2004-I-920.

PELLICORI, Oscar, "Informática y Delito", El Derecho, diario del 6/6/94;

RIQUERT, M. A.Delitos Informáticos, pag. 322 en Derecho Penal de los Negocios (Carrera, Daniel y Vázquez, H., directores), Astrea, 2005

Esther C. RODITTI, Is Self-Help a Lawful Contractual Remedy?, 21 Rutgers Computer & Tech. L.J. 431 (1995)

Harold SMITH REEVES, Property in Cyberspace, 63 U. Chi. L. Rev. 764 (1996).