DAÑO INFORMÁTICO
(ARTS. 183, 2° PÁRR. Y 184 INCS. 5° Y 6° DEL C.P. LEY 26.388)

RUBÉN E. FIGARI[1]

Sumario:

1. Consideraciones generales y antecedentes parlamentarios. 2. Tipo básico. 3. Virus informáticos. 4. Agravantes. 5. Derecho comparado.

1. Consideraciones generales y antecedentes parlamentarios

La ley 26.388 (04/06/2008 B.O. 25/06/2008 – ADLA 2008-C, 2281) que genéricamente regula los denominados "Delitos informáticos" introdujo varias modificaciones en la ley de fondo, tanto en la Parte General (art. 77) –definiendo los términos "documento", "firma" y "suscripción" e "instrumento privado" y "certificado"– como en la Parte Especial (art. 128) –pornografía infantil–; (Capítulo III Título V "Violación de secretos y de la privacidad" arts. 153, 153 bis, 155, 157, 157 bis) –todos referidos al acceso a las comunicaciones electrónicas, apoderamiento de las mismas, intercepción, publicación o al acceso a un sistema o dato informático de acceso restringido privado o de organismos públicos, o la publicación indebida de la comunicación electrónica–; (art. 173 inc. 16°) –defraudación informática–; (arts. 183, 2° párr. y 184 inc., 5° último párrafo e inc. 6°) –daño informático y sus agravantes–; (art. 197) –interrupción o entorpecimiento de comunicaciones– y (art. 255) –sustracción, alteración, ocultación, destrucción o inutilización de objetos destinados a servir de prueba.

En lo que respecta al tratamiento por parte de los legisladores, la Cámara de Diputados (Cámara de origen) había propuesto como proyecto –en lo concerniente al daño informático– los siguientes textos: Art. 12. "Incorpórase al artículo 183 del Código Penal de la Nación como segundo y tercer párrafos, los siguientes: Será reprimido con prisión de un mes a dos años el que, por cualquier medio, destruyere en todo o en parte, borrare, alterare en forma temporal o permanente, o de cualquier manera impidiere la utilización de datos o programas,

[1] Ex-Juez de la Cámara de Crimen de la Segunda Circunscripción Judicial de la Provincia de San Luis. Investigador y ensayista.

cualquiera sea el soporte en que estén contenidos durante un proceso de comunicación electrónica. La misma pena se aplicará a quien vendiere, distribuyere o de cualquier manera hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños de los descritos en el párrafo anterior, en los programas de computación o en los datos contenidos en cualquier tipo de sistema informático y de telecomunicaciones". Art. 13. –"Sustitúyese el inciso 5 del artículo 184 del Código Penal de la Nación, por el siguiente: Inciso 5: Ejecutarlo en archivos, registros, 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; o en sistemas informáticos o de bases de datos públicos". Art. 14. –"Incorpórase como inciso 6 del artículo 184 del Código Penal de la Nación, el siguiente:

Inciso 6: Ejecutarlo en sistemas informáticos relacionados con la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

En cuanto a sus fundamentos se exponía lo siguiente: "En el art. 12 el Proyecto prevé el daño producido en perjuicio de datos o programas, como agregado al art. 183 C.P. más conocido y receptado en la legislación comparada como "sabotaje informático". La cláusula se torna imprescindible ya que el código vigente sólo establece como delito el daño que recae sobre cosas tangibles, y los datos o programas de un sistema son bienes intangibles. También se introduce la figura de los "virus informáticos", al preverse la tipicidad de la distribución de programas destinados a causar cualquiera de los daños descriptos anteriormente".

La Cámara revisora, en este caso la de Senadores, proponía ciertas modificaciones en el texto. En efecto: Art. 10. –"Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Art. 11. –"Sustitúyese el artículo 184 del Código Penal, por el siguiente: Artículo 184. –La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar 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 substancias 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; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

Este texto vuelve a la Cámara de origen para en definitiva quedar plasmado como el art. 11 en la ley 26.388. No se transcriben textos del debate parlamentario ya que podría exceder los límites de este trabajo.[2]

Ante este espectro tan vasto, en esta ocasión, sólo me limitaré a dar un somero panorama sobre la interpretación que se puede realizar específicamente sobre el "daño informático" que sería el comprendido por los arts. 183, último párrafo y 184 inc. 5°, último párrafo y 6°.

Dentro de tantos intentos por definir el daño informático, en términos generales se podría decir que se trata de toda lesión o menoscabo causado a un derecho subjetivo o interés legítimo mediante la utilización de medios electrónicos destinados al tratamiento automático de la información y que concurriendo determinados presupuestos, genera responsabilidad.

"La existencia de una forma particularizada en la causación del daño –utilización de medios automáticos para el procesamiento de la información– justifica plenamente el tratamiento específico del problema encarnado por la dualidad informática-derecho, empleando una adaptación metodológica al objeto de estudio. La utilización de medios automáticos o electrónicos es el instrumento idóneo para la producción del daño informático. La expresión "medios electrónicos" pretende superar en amplitud y comprensividad a las variadas construcciones doctrinarias que referencian a computadoras, ordenadores, etc., por cuanto aparece suficientemente extensa como para receptar la evolución vertiginosa de la tecnología y la técnica, que, en breves espacios temporales, podría dejar tales expresiones obsoletas. El tratamiento informatizado de datos es propiamente el objeto de la informática, determinando el contenido de las operaciones efectuadas en utilización de sistemas de computación; es la sustancialidad de este aspecto que resulta definitiva de la informaticidad del daño, particularizándolo en relación a otros usos alternativos posibles mediante los mismos medios electrónicos".[3]

[2] Para su consulta ver www.laleyonline.com.ar *"Antecedentes parlamentarios"*.

[3] CALDERÓN, Maximiliano Rafael – HIRUELA, María del Pilar, *"Daño informático y derechos personalísimos"*, en *"Derecho de Daños. Economía. Mercado. Derechos Per-*

2. Tipo básico

En cuanto al aspecto penal, la Ley 26.388 incorpora el 2° párrafo del art. 183, referido al daño informático en estos términos: *"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"*.

En atención al primer párrafo del art. 183 se veía que el objeto material del daño está constituido por una cosa mueble o inmueble o un animal, total o parcialmente ajeno. Entonces se planteaba el problema que los bienes intangibles –software o datos almacenados en soportes magnéticos, ópticos o electrónicos– no estaban directamente enunciados en la norma y el cuestionamiento era como solucionar esta laguna normativa.

PALAZZI indicaba que una primera solución podía ser interpretar ampliamente el concepto de cosa del art. 183 lo que se vería respaldado por la evolución jurisprudencial del concepto de cosa en materia penal, que registra una apertura al considerar punibles actos cometidos sobre determinados bienes cuya naturaleza de "cosa" podía ser discutible. De esta forma se aceptaba que es posible apropiarse – y por ende destruir, los pulsos telefónicos, la señal de cable y de cualquier energía susceptible de apropiación en virtud de que el art. 2311 del C.C. reformado por la ley 17.711 otorga el carácter de cosa a la energía ([4]). Con esta última interpretación se sostuvo que la información que se encuentra en una computadora adopta la forma de energía, que podrá ser eléctrica o magnética según el soporte que la posea. "La energía magnética que está en la superficie de un disco rígido o un *diskette* –se debería agregar también un CD–, por ser apropiable, se rige, entonces por las disposiciones de las cosas. Igual criterio se aplicará a la energía eléctrica que se encuentra en la memoria de un ordenador. Ambas pueden ser alteradas por manipulación de una persona, de un programa o un virus hecho a tal efecto. Entonces, la información contenida en una computadora (ya sea en un *diskette*, en un disco rígido o en la memoria) llega a poseer la entidad suficiente para ser reputada cosa a los efectos de aplicarles las mismas disposiciones. Por otro lado la doc-

sonalísimos", GHERSI Carlos (director), Ed. Abeledo Perrot, Buenos Aires, 1999, ps. 366 y sgtes. citado por LEIVA Claudio Fabricio *"Responsabilidad por daños derivados de Internet (Reparación y prevención de los daños)"* en www.aaba.org.ar/bi22n004. htm.

[4] PALAZZI Pablo *"Delitos informáticos"*, Ed. Ad– Hoc, Buenos Aires, 2000, p. 133.

trina moderna le atribuye a la información valor en sí misma como mercancía y la posibilidad de un derecho de propiedad sobre ella".[5]

STIGLITZ-STIGLITZ, citando a FROSINI, refieren que: "la información computarizada representa una nueva forma de energía ya que comporta la utilización –para el almacenamiento, procesamiento y transmisión de los datos–, de señales electromagnéticas. Además, se señala que la energía informática es susceptible de apropiación y valuación económica", aplicando a la información computarizada el régimen de las cosas.[6] JUNYENT de SANDOVAL también sostiene esta postura, aduciendo que, la informática reúne caracteres similares a los de la energía eléctrica, ya que ésta produce trabajo explotando, accionando o poniendo en funcionamiento un dispositivo mediante una célula fotoeléctrica y, aduna que, como la energía informática implica la "intensificación de fuerzas o la potenciación del peligro ínsito en su empleo", "debe regir para ella la responsabilidad objetiva por riesgo creado".[7]

En sentido contrario a lo antes expuesto se alzaron otras voces que consideraron que los llamados "daños informáticos" no se encontraban previstos en los casos señalados por los arts. 183 y 184 del Código Penal, puesto que expresamente el articulado mencionado en primer término se refería como objeto de delito a las cosas muebles, concepto normativo definido por el artículo 2311 del Código Civil que reza: *"Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referenciadas a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación"*. Es decir, "cosa mueble" implica todo objeto detectable materialmente, transportable y susceptible de tener un valor, definición que impediría considerar a un archivo de computadora almacenado en un soporte informático como cosa mueble y, en consecuencia, como objeto del delito de daño. Sobre el punto se ha explayado la doctrina al señalar que *"El contenido intelectual o la información almacenada, es decir la idea que transmite considerada como*

[5] Ídem (ob. cit. p. 134).

[6] STIGLITZ, Gabriel A. – STIGLITZ, Rosana M., *"Responsabilidad civil por daños derivados de la informática"*; LL 1987-E – 801. En igual sentido AGOGLIA, Marta M; BORAGINA, Juan C.; MEZA, Jorge A.; *"Responsabilidad civil por daños causados por el procesamiento electrónico de datos personales"*; LL 1991-I-879 citados por FORNANGUERIA Andrea Isabel – ETIENNE Patricia Marcela *"Los virus informáticos y la protección penal de la información"* en www.sala. clacso.edu.ar

[7] JUNYENT DE SANDOVAL Beatriz *"Daños derivados de la actividad informática"* en ZAVALA DE GONZALEZ, Matilde; *"Personas, casos y cosas en el derecho de daños"*, Ed. Hammurabi, Buenos Aires, 1991, p. 221 citado por FORNANGUERIA Andrea Isabel – ETIENNE Patricia Marcela (ob. cit.).

abstracción, no puede ser comprendida en el concepto de cosa mueble... al destruir o borrar un archivo, esto es el disquete, no se daña, pues puede volver a utilizarse".[8] Por lo tanto, se consideró que ningún archivo o página web podía asimilarse al concepto de cosa, por no tratarse de un objeto corpóreo ni pasible de ser detectado materialmente, extremo que necesariamente conducía a la atipicidad de aquellas conductas dirigidas a dañar, destruir o inutilizar archivos, contenidos intelectuales o información almacenada en un soporte, diskette, disco rígido, unidad de almacenamiento extraíble o pendrive u ordenador. Así, fue entendido jurisprudencialmente por la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional en el conocido caso "Piamonti", de cuyos considerandos se advierte que "el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño (art. 183 C.P.), puesto el concepto de cosa es aplicable al soporte y no a su contenido".[9]

También se ha expuesto siguiendo la anterior postura, pero dándole otra óptica, que a la información se le atribuye un valor en sí misma como mercancía, y la posibilidad de un derecho de propiedad sobre ella. En tal sentido, FORNANGUERIA-ETIENNE entienden que se debe distinguir el concepto de información, del de energía, ya que esta última es el medio que se utiliza para plasmar la información en el soporte adecuado y recuperarla posteriormente y así como la energía humana es necesaria para escribir información en un soporte de papel, la energía electrónica es utilizada para fijar la información en la superficie magnética de un disco duro, un diskette, o la memoria de la computadora, y luego recuperarla para su lectura e interpretación. Esta alternativa la centran en la idea de que aunque el ordenador se encuentre apagado, la información contenida en los soportes del mismo continúa existiendo, del mismo modo que existe la información contenida en un archivo manual guardado en un cajón con llave.[10]

[8] FILLIA, Leonardo César – MONTELEONE, Romina – NAGER, Horacio Santiago – ROSENDE, Eduardo E. – SUEIRO, Carlos Christian *"Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)"* LL 2008-E-938 citando a CARO Rodrigo *"El archivo almacenado en soporte informático como objeto del delito de daño, artículo 183 del Código Penal"* LL 2004-A-1436. En igual sentido ROSENDE Eduardo *"Derecho Penal e informática"* Ed. Fabián Di Plácido, Buenos Aires, 2007, p. 212.

[9] Ídem citando a BROND Leonardo – BRIGNANI Sebastián *"Delitos informáticos – panorama deslindante y criterio de demarcación"* LL 2004-C-1250.

[10] FORNANGUERIA Andrea Isabel – ETIENNE Patricia Marcela (ob. cit.).

Esta laguna de la que se hablaba y su intención subsanatoria por parte de la jurisprudencia, ha sido remedada por la incorporación del segundo párrafo del art. 183. En efecto, la reforma ha ampliado los objetos de protección, tutelándose especialmente al dato, al documento, a los programas y a los sistemas informáticos como banco u objeto de ataques ilegítimos, con el fin de mantener incólume su inalterabilidad y de este modo, la afectación de tales elementos pasa a estar comprendidos dentro de la protección que anteriormente se hacía de las "cosas fungibles", con lo que –desde el punto de vista penal– el concepto de cosa se ha ampliado en forma notable, por lo que en la actualidad ya no será exclusivamente un objeto material corpóreo, sino que también se comprenderá la alteración o la destrucción de datos, documentos, programas y sistemas informáticos que tengan una calidad diferente, caracterizada principalmente por la inmaterialidad propia de tales elementos.[11]

Según TAZZA-CARRERAS en la primera parte de la norma se incrimina el llamado "sabotaje informático" consistente en la alteración o destrucción de programas o de sistemas informáticos en general de un tercero. Es constitutivo de un delito de resultado al que se puede arribar aún alterando, total o parcialmente el nuevo objeto de protección que comprende también al denominado "software" de estas nuevas tecnologías. Incluso, con la protección ampliada de esta norma, la intangibilidad de una página web en internet es alcanzada por la norma en cuestión.

Los verbos típicos son "alterare, destruyere o inutilizare". Si bien difiere del "daño común" pues se agrega el término "alterare", se entiende que no hay mucha diferencia con los conceptos previstos en el tipo penal original. "Alterar" sería modificar un archivo de datos o programa sin destruirlo completamente. En el contexto informático, "destruir o inutilizar" quiere decir borrar definitivamente sin posibilidad de recuperación. La respuesta a si esto ocurre o no en un caso concreto dependerá del sistema informático y operativo utilizado. En la mayoría de los sistemas operativos la acción de borrar no implica que el hecho se produzca indefectiblemente, pues los archivos borrados se almacenan en una carpeta conocida como basurero o *trash can.* Generalmente, para poder concluir la acción de borrado de datos el usuario debe reconfirmar el borrado para eliminar los documentos e incluso en estos casos es posible recuperarlos en algunas situaciones. Por ende, la consideración de la destrucción debe ser analizada caso por caso. Existen otras formas

[11] TAZZA Alejandro – CARRERAS Eduardo *"La protección del banco de datos personales y otros objetos de tutela penal"*, LL 2008-E-869.

de borrado mediante virus informáticos, o programas dañinos que pueden "saltearse" estas seguridades impuestas por los sistemas operativos. También cabría la posibilidad de destruir el hardware (generalmente de menor valor) con la finalidad de destruir los datos o software (de mayor valor).

El hecho que exista un sistema de *back up*, como sucede en la mayoría de las empresas en modo alguno altera el delito de daño pues la restauración requiere un esfuerzo que ya implica reparar el daño causado.[12] Por ello se afirma que no se requiere para su configuración de un daño sino que por el contrario, representa un delito de peligro y no de resultado. "Se incrimina las actividades previas que pueden llegar a provocar la producción de un resultado lesivo para los sistemas informáticos. Constituye, en definitiva, un peligro de daño sancionado en forma autónoma, aunque con idéntica penalidad".[13]

En cuanto al objeto sobre los que pueden recaer las acciones típicas son: "datos, documentos, programas o sistemas informáticos". Con ello se incrimina el denominado "sabotaje informático" consistente en la alteración o destrucción de programas o de sistemas informáticos en general de un tercero, pudiéndose arribar a dicho resultado aún alterando, total o parcialmente, el nuevo objeto de protección que comprende también al denominado "software" de estas nuevas tecnologías[14], tal como se ha dicho párrafos más arriba.

Por otra parte, además del daño informático tradicional se agrega una nueva modalidad de daño ya que se pune a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Se entiende que estos programas, como por ejemplo un *virus maker* o herramientas específicas de destrucción de datos, son potencialmente dañosas. Por consiguiente, quien de alguna manera pone en el comercio un programa de tales características, con conocimiento del daño a producir, ayuda de esta forma a cometer el delito de daño a quien usará la herramienta. No se prohíbe la existencia de estos programas, sino que penaliza a quien los venda, los distribuya o los haga circular o introduzca concretamente en un sistema informático.[15]

[12] PALAZZI Pablo *"Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007"* en *"Revista de Derecho Penal y Procesal Penal"*, Abril-Mayo 2008, Lexis Nexis.

[13] TAZZA Alejandro – CARRERAS Eduardo (ob. cit.); PALAZZI Pablo *"Análisis..."* (ob. cit. p. 20).

[14] TAZZA Alejandro – CARRERAS Eduardo (ob. cit.).

[15] PALAZZI Pablo *"Análisis..."* (ob. cit. p. 21).

Según se aprecia, en esta segunda parte de la disposición penal, la cuestión tiene vinculación con aquellas actividades referidas al manejo y manipulación de virus informáticos que pueden destruir programas existentes en tales sistemas, de modo que se sanciona tanto el acto de vender, distribuir, hacer circular, e incluso introducir tales programas que traen aparejado dicha afectación. "La modalidad de "hacker" destructivo es la contemplada por esta disposición penal, aunque también el tipo penal se conforma con algo menos, como sería la acción de vender, distribuir o hacer circular tales programas aún antes de que ellos penetren en un sistema informático".[16]

Señala PALAZZI: "En cuanto a la posibilidad de incriminar a quienes producen una herramienta que puede eventualmente usarse para crear daños informáticos, el tema se plantea con las llamadas tecnologías de doble uso, de las cuales vemos miles de ejemplos en la vida cotidiana: la fotocopiadora, la video casetera, un equipo "doblecasetera", un ipod, un disco rígido, una grabadora de dvd, el software *peer to peer*, y un largo etcétera de software y hardware que permite copiar obras intelectuales, reproducirlas, difundirlas. Tanto doctrina como jurisprudencia coinciden ampliamente en que estas tecnologías no son ilegales ni susceptibles de ser prohibidas si tienen usos sustancialmente legítimos o no infractores, aunque de paso también tengan usos no legítimos. La solución legal más razonable en estos casos es permitir la existencia de estas herramientas y solamente sancionar su uso en un caso concreto cuando este uso sea ilícito pero permitiendo que coexistan los usos legítimos. Por ende, si el programa destinado a causar daños encuentra un uso legítimo, tal uso no será ilegal, en cambio si no es posible encontrarle usos legítimos o que no produzcan daño, no se ve porque no debería prohibirse su distribución".[17]

En cierta forma la conducta que lleva a cabo el sujeto activo, se podría considerar como progresiva –aunque no necesariamente ocurra de esa forma– ya que comienza como una suerte de intrusismo –actividad que realiza el hacker– para luego pasar a ser un cracker, aunque a veces este último comienza directamente con la actividad vandálica. Esta conducta suele definirse como la de quebrar, remover o eliminar la protección de un programa de forma tal que el mismo funcione, luego de *"crackeado"*, como si hubiera sido adquirido por un usuario registrado. Se indica que una modalidad vandálica del cracking es la desarrollada por los *cyberpunks*, en la que la conducta suele venir

[16] TAZZA Alejandro – CARRERAS Eduardo (ob. cit.).
[17] PALAZZI Pablo *"Análisis..."* (ob. cit. ps. 21/22).

preordenada por el específico ánimo de destruir datos, programas o soportes informáticos. Se define al *cyberpunk* como un cracker cuyo único fin es la entrada inconsentida en sistemas informáticos –conducta típica de *hack*– mediando la corrupción de un *password* –conducta típica de crack– para destruir datos o implementar en el sistema informático un virus, o bomba lógica, que destruye a los mismos.[18]

Para algunos autores, al *sujeto activo* de los delitos informáticos se le adjudica una inteligencia y educación común superior al nivel medio, y con vastos conocimientos informáticos[19] y para denominar esta clase de sujetos se suele hablar de los antes descriptos que están caracterizados por un saber informático especial. Si bien es cierto que existen y de hecho operan personas con esas calidades, no necesariamente el delincuente informático debe poseer conocimientos profundos en la materia pues, la computación se halla tan extendida hoy en día que cualquier persona con conocimientos mínimos de informática pueda tener acceso a un ordenador y realizar un delito informático. Se menciona el caso del cajero que desvía fondos mediante el ordenador que usa para contabilizar el dinero que recibe o ingresa falsamente un monto en una cuenta o el caso del empleado de seguridad que conoce los códigos de acceso al sistema y los usa en su provecho.[20] Idéntica apreciación hace ROSENDE[21] quien cita a HERNANDEZ pues explica que en la red, más allá de los hackers, y los crackers, están los que se denominan en la jerga *underground* de la red *lamers o newvies* (novatos), *copyhackers*, "bucaneros", *script kiddie*, que demuestra los distintos grados de conocimiento que puede tener una persona para crear problemas en la red, y sin embargo, aún así, no saber nada realmente de tecnología (bucaneros).[22]

[18] MORÓN LERMA Esther *"Internet y derecho penal: "hacking" y otras conductas ilícitas en la red" "Colecc., Derecho y proceso penal N° 1"*, Aranzadi. Pamplona, 1999, ps. 32/33, citado por RIQUERT Marcelo *"Delitos informáticos"* en *"Derecho penal de los negocios"* CARRERA Daniel – VAZQUEZ Humberto (Directores) Ed. Astrea, Buenos Aires, 2004, p. 327.

[19] BUOMPADRE Jorge *"La tutela penal del sistema informático"* LL 1988 – A –985; LILLI Alicia Raquel – MASSA María Amalia *"Delitos informáticos"* LL 1986-A-832; JIJENA LEIVA Renato *"Chile, la protección penal de la intimidad y el delito informático"* Ed. Jurídica de Chile, Santiago, 1992, 110. Todos citados por PALAZZI Pablo *"Delitos..."* (ob. cit. p. 66 nota 85).

[20] PALAZZI Pablo (ob. cit. p. 67).

[21] ROSENDE Eduardo (ob. cit. p. 158).

[22] HERNÁNDEZ Claudio *"Hackers. Los piratas del chip y de Internet"* Ed. Electrónica en español, 2001, p. 35. citado por ROSENDE Eduardo (ob. cit. p. 159 nota 113).

3. Virus informáticos

Normalmente y asiduamente los mayores daños informáticos se producen mediante los denominados "virus informáticos". Se han categorizado bajo un mismo denominador diferentes programas que, si bien afectan la información, lo hacen de forma diferente, y son en realidad códigos lógicos o programas diferentes que no tienen siempre las mismas características. De esta manera son agrupados bajo el rótulo de virus informáticos, programas que no cumplen con los requisitos propios de esta clase de archivos, concluyendo que un virus informático, es algo diferente a un gusano –*worm*–, un caballo de Troya –*troyan horse*– o una bomba lógica.[23]

ROSENDE restringe el concepto en cuanto a lo que abarca el virus informático, pues considera incorrecto tratar aspectos relativos a los problemas que platean las bombas lógicas, los gusanos y los caballos de Troya, pues estos archivos exceden las capacidades informáticas de lo que se denomina virus, mientras que a su vez les falta ciertas características propias de esta clase de amenaza informática, sin perjuicio de que se hayan creado programas que permitan agrupar distintas características de estas cuatro categorías, por ello considera más correcto hablar de "amenazas lógico informático" que permite embolsar tanto a los virus informáticos, como los gusanos, los caballo de Troya y las bombas lógicas.[24]

Entonces, los virus informáticos son pequeños programas cuya mayor cualidad es la capacidad de autorreproducirse, mediante su ejecución y copiado en un archivo de una computadora siendo una de sus posibles consecuencias el borrado de programas y archivos, la desestabilización del sistema operativo, la recarga de los recursos del sistema, o la memoria, o simplemente la inclusión de mensajes de chistes, realizando todas estas actividades sin la participación de un usuario y con el desconocimiento de éste, utilizando solamente los parámetros de su programación[25] y es esta capacidad de autoreproducción la que diferencia a los virus informáticos de los caballos de Troya y las bombas lógicas.[26]

Un programa gusano, recibe su designación por la forma en que se desliza en y fuera de una red de computación y como en la mayoría de los virus, un

[23] ROSENDE Eduardo (ob. cit. p. 133).
[24] Ídem (ob. cit. p. 135).
[25] PALAZZI Pablo (ob. cit. p. 145).
[26] ROSENDE Eduardo (ob. cit. p. 136).

programa gusano es sólo peligroso cuando es diseñado para realizar alguna función particular y cuando uno de esos programas se escribe para realizar una función negativa, el programa se mueve a través de una red y desactiva las computadoras helando teclados y pantallas, llenando la memoria o reduciendo la velocidad. Los gusanos o *worms* son los archivos que más semejanza presentan con los virus por su autoreproducción, pero con la diferencia que éstos no producen efectos destructivos en su versión pura, sino que su objetivo es colapsar el sistema o ancho de banda, mediante su replicación constante.

Las llamadas "bombas lógicas" liberan su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora específica o cuando se teclea una combinación de letras. La condición puede ser la llegada de una fecha –bomba de tiempo–, una combinación de teclas o una determinada técnica. Si no se produce ese evento disparador, las bombas lógicas permanecen ocultas y hasta pueden no activarse.

Otra modalidad es el denominado "caballo de Troya" que son programas destructivos encubiertos, aparecen en forma de juego, utilidades y adjuntos de correos electrónicos y una vez abiertos actúan de una manera muy distinta a la esperada, algunos son sólo molestos y envían correo electrónico a todos los nombres incluidos en la libreta de direcciones, otros causan daños graves, a punto de robar contraseñas y archivos. A diferencia de los virus, los caballos de Troya no se autorreproducen. No se va a entrar en detalle del porqué se denominan así pues se sabe que viene del término caballo de Troya referido en el mítico relato de Homero.[27]

Se ha dicho que los virus informáticos no afectan –en su gran mayoría– directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contiene un código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general, los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

De esta manera se podría estructurar una clasificación progresiva de acuerdo a la siguientes pautas: a) *Daño Implícito*: se trata del conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar

[27] Ídem (ob. cit. ps. 136/142).

su accionar y propagación. Aquí se debe considerar el entorno en el que se desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado –como un aparato biomédico– puede causar un gran daño. b) *Daño Explícito*: es el que produce la rutina de daño del virus. Y con respecto al modo y cantidad de daño, se pueden manifestar como: 1) *Daños triviales*: es decir, los que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, muy poco tiempo. 2) *Daños menores*: los que ocasionan una pérdida de la funcionalidad de las aplicaciones. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas. 3) *Daños moderados*: los que el virus provoca al formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizar la última copia de seguridad que se ha hecho y reinstalar el sistema operativo. 4) *Daños mayores*: algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas. Puede que se llegue a encontrar una copia de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad. 5) *Daños severos*: son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado el sistema y 5) *Daños ilimitados:* en este caso el virus "abre puertas" del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.[28]

Hecho un somero panorama sobre algunos de los modos más corrientes en la forma que se producen los daños más frecuentes en la parte informática y ya apartándose de la cuestión operativa y volviendo a entrar en la parte jurídica, se puede afirmar, que desde el aspecto subjetivo al igual que en el daño convencional, se trata de un tipo que requiere dolo directo, sin necesidad de una ultra finalidad o motivos específicos.

Lo concreto y real, es que a partir de la redacción de esta nueva fórmula, se puede decir que se instala el daño informático en nuestra legislación y se alejan todas las controversias jurisprudenciales que se produjeron sobre el particular.

[28] www.segu-info.com.ar/virus/danios. htm.

4. Agravantes

El art. 11 de la ley 26.388 realiza un agregado en el inc. 5° del art. 184 aludiendo a los *datos, documentos, programas o sistemas informáticos públicos.*

Esto está referido tanto para el daño informático propiamente dicho como a la introducción de virus informáticos en tales sistemas. "El inciso quinto de este articulado funda el agravante en el hecho de que hay un interés de toda la colectividad en la preservación de la intangibilidad de los objetos que se mencionan en el inciso. De ahí la protección mayor que la ley ha querido dispensarles estatuyendo una pena más grave para el daño de que ellas puedan ser objeto. El daño se agrava aquí por la naturaleza y el destino y la situación de la cosa... Creemos que la calidad de "públicos" en cuanto se refiere a los datos, documentos, programas o sistemas informáticos, debe ser entendido en su vinculación con la naturaleza de la información y con la titularidad oficial de su pertenencia o almacenamiento".[29]

Y se introduce el inc. 6° que agrava el daño al: *"Ejecutarlo en sistemas informáticos destinados a la prestación de servicio de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".*

En este inciso se contempla el sistema informático como objeto de protección penal y a la información allí contenida, en la medida que revistan una finalidad específica y calificada por estar relacionada con la prestación de servicios de salud, comunicación, provisión, transporte de energía, medios de transporte u otros servicios públicos y se aplica el agravante cuando el daño se ocasione en programas o sistemas informáticos públicos, pertenecientes al Estado –Nacional, Provincial o Municipal– mientras que será de aplicación el inciso 6° cuando el daño afecte al sistema informático de alguna de las prestaciones de servicio calificada por el mismo articulado ya que, en el primer supuesto se agrava por la naturaleza y pertenencia de la información, mientras que en el segundo, por la calidad del servicio que presta la entidad afectada, aunque esta última sea de carácter privado.[30]

[29] TAZZA Alejandro – CARRERAS Eduardo (ob. cit.).
[30] Ídem (ob. cit.).

5. Derecho comparado

En Estados Unidos se ha tipificado una figura de destrucción de datos y sistemas informáticos y la Ley Federal de delitos informáticos, denominada *Computer Fraud and Abuse Act* de 1986, contempla en la Sección (a).5 la alteración, daño o destrucción de información como un delito autónomo.

El Código Penal alemán en 1986 introduce en el §303. a el siguiente texto: "Alteración de datos. (1) Quien borre, suprima, inutilice, o cambie antijurídicamente datos (§202 a, inciso 2), será castigado con pena privativa de la libertad hasta dos años o con multa. (2) La tentativa es punible". El §303. b. "Sabotaje de computadoras (1) Quien perturba un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad para 1.cometer un hecho según el §303 a, inciso 1 ó 2, destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos será castigado con pena privativa de la libertad hasta cinco años o con multa. (2) La tentativa es punible".-

El Código Penal de Austria (1987) en el §126. a dispone que: "1. Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca en todo o en parte, de disponibilidad, será castigado con pena privativa de libertad de hasta seis meses o con pena de multa de hasta 360 días-multa".

Francia con la ley N° 88-19 del 5 de enero de 1988 incluyó en su Código Penal varios delitos informáticos. Entre ellos, se encuentran la figura del art. 462-4 referida a la destrucción de datos que, establecía que "Quien, intencionalmente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de los dos penas". Con la reforma penal de 1992, este artículo quedó ubicado en el art. 323-1, con la siguiente modificación: "Se penaliza a quien al acceder a un ordenador de manera fraudulenta, suprima o modifique los datos allí almacenados".

El Código Penal italiano (1993) en el art. 392 incluye la alteración, modificación o destrucción total o parcial de programas de computación y el daño a la operación de un sistema telemático o informático. El artículo 420 del Código Penal, referido a atentados contra sistemas de instalaciones públicas, ha sido

también modificado. Actualmente cualquiera que realice un acto con la intención de dañar o destruir sistemas informáticos o telemáticos de instalaciones públicas o sus datos, información o programas puede ser castigado con prisión de uno a cuatro años. En casos de consumación del delito (destrucción o daño a los datos) la pena se eleva de tres a ocho años.

El Código Penal español (1995) contempla en el art. 264.1 "Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el Artículo anterior, si concurriere alguno de los supuestos siguientes: ... 2. La misma pena se impondrá 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".

En Latinoamérica varios países han legislado este tipo de delitos, entre otros: Chile (Ley 19.223 de 1993), Bolivia (Ley 1.768 de 1997), Paraguay (reforma al CP en 1997), Perú (reforma al CP en 2000), Colombia (Ley 679 de 2001 sobre pornografía infantil en redes globales), Costa Rica (Leyes 8.131 y 8.148 de 2001), Venezuela (Ley Especial de 2001) y México (Código Penal Federal).–