EDITORIAL ASTREA

*MP3 y virus informáticos**

Por Leonardo G. Brond, Sebastián Galar, Sebastián Brignani y María A. Castella

1. Introducción

a) Generalidades

El propósito de este trabajo es relacionar dos áreas del derecho: el derecho penal (cuyo contenido está claramente determinado) y el derecho informático (hasta ahora de contenido borroso, apenas insinuado).

En 1983, la Organización para la Cooperación y Desarrollo Económicos definió al *delito informático* como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos. Esta definición, lejos de ser de aceptación general, presenta varios problemas, como veremos más adelante.

Nuestro Código Penal, por su parte, data de 1921. En esa época no existían los bienes inmateriales (datos, programas de computación, etc.) con la extensión que los conocemos hoy. En aquellos tiempos, el legislador no previó, ni pudo prever los denominados "delitos informáticos" que se presentan hoy.

Acorde con esta interpretación subjetiva de la ley, junto con los principios aceptados por la dogmática penal (tipicidad, prohibición de la analogía), sólo de *lege ferenda* se podría sostener la punibilidad de estos delitos. Como veremos más adelante, sin embargo, las aguas no están tan mansas como parecen.

Aun existiendo tipos penales que regulen las conductas en cuestión, hay dificultades: *1*) el lugar de comisión y la ley aplicable; *2*) los autores de estos delitos suelen ser menores de edad (o niños) –incapaces de culpabilidad– pero con una inteligencia y conocimiento notoriamente superiores al de cualquier integrante de una fiscalía, y *3*) la tecnología del delincuente informático suele ser también más avanzada a la de los órganos de persecución[1].

Internet ha contribuido también con sus ventajas y desventajas, entre los problemas que se plantean encontramos los siguientes:

1) El régimen de registros de nombres de dominio a nivel internacional y en nuestro país, su ocupación abusiva.

2) El principio de libertad de expresión y su vinculación con la libertad de contenidos y la posibilidad de censura previa.

3) Los delitos cometidos a través de Internet.

4) La responsabilidad de los diferentes proveedores que intervienen en la red.

5) La afectación de los derechos a la propiedad intelectual de los autores, compositores e intérpretes, en especial, el fenómeno MP3.

---

* *Bibliografía*: Palazzi, Pablo A., *Delitos informáticos*, Bs. As., Ad-Hoc, 2000.

[1] Durrieu, Roberto - Lo Prete, Justo, *Delitos informáticos*, *LL*, 2002-A-1287.

6) La afectación de la privacidad de los individuos.

7) La protección de datos personales.

8) La defensa legal de los sitios *web*.

9) La introducción de virus informáticos.

b) Precisiones terminológicas

Si bien el problema de los virus informáticos será tratado más adelante, queremos desde ya dejar aclarado el concepto de "delitos informáticos"[2] dada la ambigüedad del término, delimitando así el objeto de investigación.

Podemos decir que cada autor tiene su propio concepto de "delito informático". Además, hay otras expresiones en nuestro idioma, provenientes de autores extranjeros: "delitos de computadora", "delitos cibernéticos", "delitos computacionales". Hay otra expresión rayana a estos términos: "delitos comunes cometidos por medios informáticos". Finalmente, están los delitos comunes más antiguos que no se cometen por medios informáticos, pero que se relacionan de alguna manera con la computadora (cuando p.ej., la computadora es objeto de daño o de robo).

Delimitamos aquí el problema del daño informático de otros delitos, cuales son los delitos comunes cometidos por medios comunes y los delitos comunes cometidos por medios informáticos.

1) Están los *delitos comunes cometidos por medios comunes*, pero donde interviene la computadora. Si tomamos el ejemplo del robo de una computadora. Esto es un delito de robo. La computadora es el objeto. En este caso, robar una computadora es exactamente lo mismo que robar un televisor de lujo, o una bolsa con piedras preciosas. A la inversa: decir que esto se trata de un delito informático es algo tan absurdo, como decir que un hurto, donde el autor debe subir una escalera de dos escalones, es un "hurto con escalamiento".

2) Luego vienen los *delitos comunes cometidos por medios informáticos*. Por ejemplo: violación de secretos; calumnias o injurias por Internet (arts. 109 a 117, Cód. Penal); exhibición obscena; instigación a cometer delitos (art. 209); instigación al suicidio (art. 83); apología del delito; tráfico de menores; comercio de estupefacientes; extorsión (art. 168); homicidio (art. 79). Merece especial atención el delito de estafa (art. 172), p.ej., la compra de bienes a través de Internet, donde el comprador utiliza una tarjeta falsa, o de un tercero. También es posible que el vendedor engañe vendiendo un objeto diferente al ofrecido.

Otro delito común cometido por medios informáticos es la intimidación pública (art. 211). Esto tiene especial importancia en la macrocriminalidad terrorista[3], una monstruosa forma de criminalidad mediante la cual murieron aproximadamente 3.200 personas en Nueva York, el 11 de septiembre de 2001.

---

[2] Durrieu - Lo Prete, *Delitos informáticos*, *LL*, 2002-A-1286.

[3] Naucke, Wolfgang, *Strafrecht. Eine einführung*, 10ª ed., Frankfurt, Luchterhand, 2002, § 1, núm. marg. 196 y 207 p. 49 y 53. Una reseña a esta obra puede verse en la revista "Nueva Doctrina Penal 2001/B", Bs. As., Editores del Puerto, 2002, p. 743 a 749.

Observa Creus que el terrorismo no es un delito, es la caracterización de una particular finalidad de una serie de delitos conformados en tipos autónomos. En la generalidad de los casos, persigue la imposición de una determinada idea (ideología política, religiosa, pureza racial, etc.) mediante el temor[4].

Si por un procedimiento electrónico de difusión masiva (como Internet) se "amenaza con la comisión de un delito de peligro común", se penetra en el tipo. Se podrá discutir si se trata de un "medio material" enunciado por aquél, pero no hay dudas de que se puede actuar con el procedimiento electrónico para "infundir temor o suscitar tumultos o desórdenes".

Otro delito común cometido por medios informáticos es la piratería (art. 72, ley 11.723), dado que sólo se necesita un disquete virgen y una computadora para consumar este delito. La acción típica se realiza rápida y ocultamente. No se dejan huellas de su ejecución. La copia doméstica (privada) de *back up* no es delito, mientras no se la emplee en otras computadoras. La copia utilizada en otras computadoras tornan discutible la cuestión.

En este catálogo se ubica el delito de daño común por medios informáticos, en la siguiente forma: introducir un virus, que destruye el *hardware* de una computadora ajena. Este delito es un daño en la computadora en tanto cosa, porque se destruye, por ejemplo, el disco rígido.

Todos estos son delitos comunes por medios informáticos, aunque para algunos autores sean "delitos informáticos". En general, puede sostenerse que los delitos comunes pueden cometerse por medios informáticos mientras no se trate de los llamados "delitos de propia mano" (violación, estupro, abuso deshonesto).

3) Luego viene el delito de daño informático. Este es el supuesto, en que el virus destruye el *software*. Este delito se lo conoce también como "alteración de datos" en el derecho comparado.

Con respecto a los virus, proponemos el siguiente "criterio de demarcación"[5]: distinguir entre virus que atacan los datos y los programas, por un lado, y virus que atacan la computadora en tanto "cosa", por el otro. Si el virus ataca ambos objetos, la punibilidad puede entrar en cuestión debido al daño en la cosa material.

Sin embargo, la doctrina predominante no comparte este criterio, porque considera –como la mayoría de los virus aparecidos en las últimas décadas del siglo XX– que el virus sólo destruye el *software*, pero no el *hardware*.

2. El fenómeno MP3

a) Historia del formato MP3

La música a través de la historia del hombre, ha sido un vehículo para transmitir emociones y estados de ánimo. Por eso la música estuvo siempre presente en

[4] Creus, Carlos, *La persecución del terrorismo en la legislación penal argentina y el "delito cibernético"*, *JA*, 1999-IV-980.

[5] La expresión está tomada de Popper (Popper, Karl R., *Conjeturas y refutaciones. El desarrollo del conocimiento científico*, Barcelona, Paidós, 1994).

todo tipo de sociedad con el debido reconocimiento a quienes la crean y la interpretan[6].

Con el avance de la civilización, ese reconocimiento tiene que luchar por su norma positiva que lo proteja y tiene que luchar contra aquellos, que sin crear música intentan obtener ganancias. En su momento, el gran problema fue el disco de vinilo, luego la cinta del *cassette*, más tarde el CD. Hoy es el fenómeno MP3.

El nuevo formato MP3 marcó un hito en la computación y en la música, además de generar trabajo para los juristas que aplican derecho.

Este fenómeno, que fue creado en la década del 80, marcó el comienzo de una gran polémica que se despertaría masivamente varios años después y que aún persiste. Antes de asomarnos a la polémica, sin embargo, es conveniente dar algunos detalles del formato MP3.

1) *Ventajas del formato MP3 frente al disco compacto*. Uno de los nuevos problemas del derecho, vinculado con el avance de la computación y su nuevo vehículo, la Internet *world wide*, es el tema de los derechos intelectuales. Vinculado con esto último encontramos el auge de la transmisión de música a través de la red, cuestión que afectó a las grandes compañías discográficas y a algunos autores de obras musicales.

La música de un CD contiene pistas a las cuales reconoce la PC con la extensión de un CD.

El archivo MP3 (también denominado MPEG *Audio Layer*) es un formato digital de audio, con una altísima fidelidad, que si bien es menor a la del CD, tal diferencia de fidelidad no es audible al oído humano. Esto se debe a que al comprimir archivos de CD a MP3, sólo se pierden *bits* de datos en frecuencias no audibles, pero que ocupan tanto espacio de almacenamiento como los *bits* de datos en frecuencias audibles. Mediante esta compresión se reduce notoriamente el espacio de almacenamiento, p.ej., una canción completa de una duración de 3 minutos, que en CD ocupa 32 MB, puede comprimirse a formato MP3 ocupando sólo 3 MB, sin que el oído humano registre una pérdida significativa[7].

Una ventaja del formato MP3, entonces, es la reducción del espacio de almacenamiento. La otra ventaja es la mayor facilidad y velocidad de su transmisión.

2) *Los aparatos reproductores de MP3*. A las dos ventajas anteriormente señaladas (reducción del espacio de almacenamiento y mayor velocidad de transmisión) debemos agregar una tercera: la utilización de aparatos reproductores de MP3; ello permite prescindir de la PC. Además, está la posibilidad de convertir los archivos de MP3 a pistas de audio en un CD nuevamente.

El caso más escandaloso fue el reproductor de MP3 “RIO de Diamond”, que era un aparato similar al walkman de Sony. Hoy en día este aparato está disponible

[6] Ossa Rojas, Claudio, *El fenómeno del MP3 y el caso Napster*, “Revista de Derecho Informático Alfa-Redi”, extraído del sitio: http://www.alfa-redi.org/revista/data/33-7.asp.

[7] Ossa Rojas, *El fenómeno del MP3 y el caso Napster* y en Vibes, Federico P. - Alesina, Juan C., *El caso “Napster” ¿Un fallo paradigmático?*, *LL*, 2001-D-165.

en el mercado, a pesar de que los mismos que demandaron a Napster habían demandado a la compañía Diamond Multimedia[8].

b) El caso "Napster"

1) *Origen y funcionamiento*. La historia comenzó cuando un ex-estudiante de informática hizo un programa para compartir la música de sus amigos. El estudiante se llama Shawn Fanning, y tenía tan solo 17 años al momento de la creación del *software*[9], el sitio se llamaba *Napster*.

Es de destacar, sin embargo, que a la fecha de la creación de este *software* ya había descargas en otros sitios de Internet que tampoco abonaban derechos al propietario de la obra en la generalidad de los casos.

Con todo, el *software* Napster facilitó de modo creciente la obtención y descarga de archivos MP3, debido a que se gestó una gran comunidad de usuarios aglutinados con la única finalidad de obtener música gratis. Se dijo en aquel entonces, que Napster era "otra caja de Pandora en la red"[10].

Este programa era un motor de búsqueda de archivos musicales en directorios a compartir de las PC de los diversos usuarios, y que facilitaba su descarga o transferencia de los archivos de una PC a otra.

Cabe aclarar, que Napster sólo facilitaba el acercamiento y la descarga, pero no almacenaba temas, sino que eran los integrantes de la comunidad Napster quienes los almacenaban y permitían su descarga por otro usuario. Esta tecnología se denomina *peer to peer* o "p2p", que permite buscar archivos en los discos duros de los ordenadores conectados a la red de distribución. Es decir, ya no se trata de información de ordenadores que actúan como servidores (los que son fácilmente identificables y por lo tanto responsables naturales de lo que se difunde en la red), sino que se posee un universo ilimitado de PC para copiar archivos.

Una observación que también es necesaria: el formato MP3 no fue la primer tecnología que competía con el formato CD. Antes del formato MP3 estuvo en boga el formato DAT (sistema de grabación de cintas digitales), en 1986[11].

2) *El juicio contra Napster*. El desmedido número de copias de temas musicales que generó el *software* Napster provocó que la RIAA (*Recording Industry Association of America*), entidad que une a las empresas discográficas de Estados Unidos de América demandara a "Napster.com".

Debido a que no se pagaban los derechos de autores y productores, la RIAA solicitó que se prohíba el funcionamiento de Napster, como así también, el pago de

[8] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.

[9] Fernández Delpech, Horacio, *Internet: su problemática jurídica*, Bs. As., Abeledo-Perrot, 2001, p. 191 y en Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.

[10] *Otra caja de Pandora en la red*, La Nación, 2/3/00 y en *La batalla legal en torno del caso Napster*, El Cronista, 7/8/00.

[11] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.

derechos *copyright* por los temas descargados. La RIAA exigió 100.000 dólares por cada descarga de un tema protegido por las leyes del *copyright* [12].

A esta demanda presentada por la RIAA se unieron otros litisconsortes (varios intérpretes). Otros intérpretes presentaron otras demandas.

3) *Argumentos en contra de Napster*. Uno de los argumentos en contra de Napster.com, que utilizó la RIAA para fundar su demanda, fue la falta de consentimiento de los titulares de los derechos para la distribución de su música, agregando que esta actividad de Napster atentaba contra la industria musical y era violatoria de los derechos de propiedad intelectual.

Dicho gráficamente: en Napster se descargaban más de 14.000 temas musicales por minuto (aproximadamente más de 20 millones de canciones diarias).

También sostuvo la RIAA, que estos programas sólo fomentan la reproducción de copias ilícitas de música y la violación de los derechos de autores e intérpretes musicales[13]. Las actividades de Napster provocaban un descenso en las ventas y frenaban el desarrollo de la música de pago por Internet, sobre todo entre estudiantes de colegios y universidades[14].

4) *Argumentos a favor de Napster*. El principal abogado de Napster, David Boies, tenía como argumentos, primero que su accionar no era ilícito ya que no distribuye ni almacena música (p2p) y que el intercambio se efectúa en forma directa por usuarios que comparten archivos a título personal, y sin ánimo de lucro. Esta situación, sostuvo Napster, estaba contemplada en el acta de reproducción hogareña de audio de los Estados Unidos de América de 1992 (*Audio Home Recording Act*)[15]. Dado que Napster sólo se limitaba a poner el programa a disposición de sus clientes, no se la podía hacer responsable de los delitos que pudieran cometer los usuarios[16].

El otro argumento, expresado por Boies en la CNN, decía que: “El usuario individual tiene un derecho absoluto a compartir música. El problema es que la RIAA parece determinada a matar este nuevo medio”[17].

5) *Desarrollo posterior del juicio*. El 26 de julio de 2000, la jueza federal Marylin Hall Patel de San Francisco, hizo lugar a la demanda de la RIAA ordenando a Napster el cese de su actuación antes del 28 de julio.

El fallo expresa: “ordénese a Napster no copiar, ayudar, o facilitar o contribuir a la reproducción del material amparado por las leyes de derechos de autor, del cual el demandante es propietario”[18]. Señaló a su vez que, como Napster creó el *software* para compartir música, asimismo tiene la obligación de crear uno nuevo para evitar que los usuarios copien canciones protegidas[19]. No obstante, la jueza advirtió a la

[12] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[13] Fernández Delpech, *Internet: su problemática jurídica*, p. 192.
[14] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[15] Fernández Delpech, *Internet: su problemática jurídica*, p. 192 y 193.
[16] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[17] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[18] Fernández Delpech, *Internet: su problemática jurídica*, p. 193.
[19] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.

RIAA, que de perder el caso, tendrían que pagar 5 millones de dólares a Napster como indemnización.

A pesar de la sentencia de primera instancia, la demandada consiguió que no se suspendieran sus servicios durante la tramitación de la apelación.

El 27 de julio, Napster solicitó a la Novena Corte del Circuito de Apelaciones en San Francisco la suspensión del cumplimiento del fallo, por ser técnicamente imposible su cumplimiento. En esto es de destacar la hábil defensa del abogado de Napster quien señaló: "si el fallo de la Corte requiere bloquear un grupo no identificado de canciones, es imposible que podamos cumplir con esa sentencia sin tener que quitar los componentes más importantes de nuestro servicio".

El 28 de julio, aquella misma Corte hizo lugar a la suspensión del fallo de la jueza, y estableció que podría seguir funcionando hasta la vista de causa fijada para el 2 de octubre del 2000, debido a que debía analizarse el caso con mayor profundidad. Su resolución aparecería recién en febrero de 2001. Los abogados de Napster habían hecho "cuestionamientos sustanciales".

6) *Un Napster "aburguesado"*. Hasta ahora habíamos conocido a Napster como un programa muy moderno, crítico de la situación económica existente, y cuya comunidad se fundaba en fuertes relaciones de solidaridad entre sus miembros. Posiblemente pueda identificarse a Napster con la filosofía de una cooperativa. Gracias a Napster, la música llegó con buena intensidad a mucha gente, que quizás no hubiera podido comprar esa música durante toda su vida. Los abogados de Napster defendieron esta versión aun dentro del juicio. Sin embargo, la etapa crítica de Napster estaba llegando a su fin.

Sorpresivamente, el 31 de marzo de 2000, Bertelsmann, el gigante conglomerado alemán dedicado a los medios, informó que aportaría capital a Napster para desarrollar un sistema p2p que permitiera el intercambio seguro de archivos de música y su uso comercial. Anunció también, el desistimiento de la demanda ni bien el sistema entre en funcionamiento.

Los términos de este acuerdo apuntan a que Bertelsmann apoyaría a Napster. Pero Napster tendría que cobrar a cada usuario una mensualidad de 5 dólares para mantener tal calidad. Esto compensaría a los autores, artistas, productores y sellos discográficos cada vez que una canción sea bajada de la *web*. Al acuerdo de Bertelsmann se agregaron otras discográficas.

En febrero de 2001, Napster realizó una propuesta en la cual ofrecía 150 millones de dólares anuales durante cinco años a Sony, Warner, BMG, EMI y Universal junto con otros 50 millones de dólares adicionales destinados a sellos. Para marzo de 2001 ya encontramos un Napster "aburguesado"[20].

El dinero ofrecido iba a provenir de un servicio pago que Napster quería lanzar si las compañías discográficas le permitían usar sus canciones. Esto parece poco si tenemos en cuenta que la industria discográfica maneja 40 millones de dólares al año.

[20] *Napster firmó un acuerdo y ya no ofrecerá música gratis en Internet*, Clarín, 2/11/00.

La empresa discográfica BMG firmó un acuerdo de cooperación con Napster, acordando el pago de un precio por los usuarios. Además, esta compañía discográfica retiró su demanda.

Los usuarios de Napser sin embargo, no estaban muy conformes con este proceso de "aburguesamiento". Así las cosas, muchos de los usuarios que en un principio estaban vinculados por la solidaridad, se trasladaron a otros sitios de Internet, que si bien no son iguales que el Napster antiguo, tampoco son fundamentalmente distintos de éste.

7) *El fallo de la Corte*. En el mes de febrero del 2001, la Novena Corte del Circuito de Apelaciones dictó un fallo de 59 carillas, estableciendo que existían violaciones a los derechos de autor por los usuarios de Napster y que esta última ayudó y alentó esa infracción.

El fallo expresa: "Napster es un infractor de segundo grado de las violaciones de los derechos de autor"[21]. A continuación se transcriben las partes pertinentes del fallo[22]:

"Los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital– vulneran el derecho de distribución que tienen las compañías fonográficas –17 U.S.C., art. 106.1– al enviar música protegida por el derecho de autor, bajo el formato MP3, a un índice de búsqueda de acceso irrestricto –*uploading*– con el fin de que otros la copien" (párr. 1°).

"Los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital– lesionan el derecho de reproducción que tienen las compañías fonográficas –17 U.S.C., art. 106.3–, al bajar archivos que contienen música protegida por el derecho de autor –*downloading*– con fines de copia y reproducción" (párr. 2°).

"Revisten carácter comercial las actividades de envío a un índice de búsqueda de acceso irrestricto –*uploading*– y bajada con fines de copia y reproducción –*downloading*– de fonogramas protegidos por el derecho de autor que realizan los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital bajo el formato MP3–, puesto que no se circunscriben a un ámbito de uso personal, recibiendo cada usuario en forma gratuita algo que en condiciones normales debería abonar" (párr. 3°).

"Configuran actividades comerciales el envío a un índice de búsqueda de acceso irrestricto –*uploading*– y la bajada con fines de copia y reproducción –*downloading*– de fonogramas protegidos por el derecho de autor que realizan los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital bajo el formato MP3–, aun cuando no obtengan beneficio económico directo, pues tal actividad tiende a evitar el gasto que conllevaría adquirir las obras legítimas, lo que supone una ventaja patrimonial indirecta" (párr. 4°).

[21] Fernández Delpech, *Internet: su problemática jurídica*, p. 194.

[22] Corte de Apelaciones, Noveno Circuito, Estados Unidos, 12/2/01, "A&M Records Inc. y otros c/Napster Inc.", *LL*, 2001-D-169 comentado por Vibes - Alesina, *El caso "Napster" ¿Un fallo paradigmático?*, *LL*, 2001-D-167.

"El envío a un índice de búsqueda de acceso irrestricto –*uploading*– y la bajada con fines de copia y reproducción –*downloading*– de fonogramas protegidos por el derecho de autor que realizan los usuarios del sistema Napster –transmisión y retención de sonidos grabados mediante tecnología digital en formato MP3–, no configura uso legítimo sino infracción al régimen de propiedad intelectual, pues tal actividad importa copia total de dichas obras –no hay transformación, sino mera retransmisión–, es de carácter comercial y apta para reducir la venta de los originales y generar barreras al ingreso de los sellos discográficos en venta por Internet" (párr. 5°).

"La bajada con fines de copia y reproducción de fonogramas protegidos por el derecho de autor que realizan los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital bajo el formato MP3–, a fin de evaluar si adquieren o no una obra original –*sampling*–, no configura uso legítimo sino infracción al régimen de propiedad intelectual, dado que las compañías fonográficas, a diferencia de Napster Inc., cobran regalías por su exhibición a los sitios de Internet y sólo permiten muestras parciales o canciones enteras programadas para permanecer un lapso corto en la computadora del usuario" (párr. 6°).

"La bajada con fines de copia y reproducción de fonogramas protegidos por el derecho de autor que realizan los usuarios del sistema Napster –diseñado para transmitir y retener sonidos grabados empleando tecnología digital, bajo el formato MP3–, a fin de contar con una copia de uso personal respecto de un original que poseen de antemano –*spaceshifting*– no configura uso legítimo sino infracción al régimen de propiedad intelectual, ya que tal método involucra simultáneamente la distribución al público de material protegido por el derecho de autor, excediendo la copia obtenida el ámbito del usuario que la realiza" (párr. 7°).

"Napster Inc. es responsable por violación al régimen de propiedad intelectual, en carácter de infractor contributivo –esto es, por fomentar y asistir a sabiendas a los infractores principales– respecto del envío a un índice de búsqueda de acceso irrestricto –*uploading*– y la bajada con fines de copia y reproducción –*downloading*– de fonogramas protegidos por el derecho de autor que realizan sus usuarios bajo el formato MP3, pues no podía ignorar que se estaba intercambiando material protegido y contaba con los medios necesarios para bloquear el acceso de sus usuarios a dicho material" (párr. 8°).

"Debe atribuirse a Napster Inc. responsabilidad vicaria –al no haber ejercido su facultad de supervisión sobre el infractor principal, obteniendo un beneficio económico directo del hecho ilícito– por la violación al régimen de propiedad intelectual que perpetran sus usuarios mediante el envío a un índice de búsqueda de acceso irrestricto –*uploading*– y la bajada con fines de copia y reproducción –*downloading*– de fonogramas protegidos por el derecho de autor bajo el formato MP3, pues dicha empresa lucra con tal actividad y cuenta con los medios necesarios para localizar el material protegido e interrumpir el acceso a sus usuarios" (párr. 10).

"La prohibición de accionar judicialmente por infracción al derecho de autor con sustento en la ley de reproducción hogareña de fonogramas –*Audio Home Recording Act*– cuando se discute sobre la fabricación, importación o distribución de música por medios digitales –17 U.S.C. 1008– es inaplicable a la bajada de archivos en formato MP3, con fines de copia y reproducción, dado que la computadora personal

y su disco rígido no constituyen equipos de grabación digital en los términos del régimen citado" (párr. 11).

"La contribución de las compañías fonográficas al desarrollo de los archivos MP3 –diseñados para transmitir y retener sonidos grabados empleando tecnología digital– no puede interpretarse como renuncia a la protección que emana de la titularidad del derecho de autor por la música que graban, distribuyen y venden, dado que con tal acción se limitaron a fomentar proyectos... y diseño de artefactos para la ejecución de esa clase de archivos" (párr. 12).

"La oposición de los sellos discográficos al *uploading* –envío de fonogramas protegidos por el derecho de autor a un índice de búsqueda de acceso irrestricto para que otros los copien– y el *downloading* –bajada de tales archivos con fines de copia y reproducción– que realizan los usuarios del sistema Napster bajo el formato MP3, no configura un ejercicio abusivo del derecho de autor, pues no persiguen controlar áreas ajenas al monopolio que brinda tal derecho, sino preservar facultades inherentes al mismo –17 U.S.C., art. 106–, cuales son la reproducción y distribución de dichas obras en mercados y con soportes alternativos" (párr. 13).

"Es procedente la orden judicial preliminar –medida de carácter cautelar– tendiente a que Napster Inc. haga todo lo posible por impedir el *uploading* –envío de fonogramas protegidos por el derecho de autor a un índice de búsqueda de acceso irrestricto para que otros los copien– y el *downloading* –bajada de tales archivos con fines de copia y reproducción– que realizan sus usuarios bajo el formato MP3, debiendo los sellos discográficos accionantes indicar las obras musicales cuya titularidad ostentan, a fin de facilitar su remoción del índice de búsqueda" (párr. 14).

"La oposición de los sellos discográficos al *uploading* –envío de fonogramas protegidos por el derecho de autor a un índice de búsqueda de acceso irrestricto para que otros los copien– y el *downloading* –bajada de tales archivos con fines de copia y reproducción– que realizan los usuarios del sistema Napster bajo el formato MP3, no atenta contra la libertad de publicación de Napster Inc. y el derecho de sus usuarios a intercambiar información –Primera Enmienda de la Constitución norteamericana–, dado que dicha actividad es contraria al régimen de propiedad intelectual, por lo que no merece protección legal" (párr. 15).

El 6 de marzo del 2001, el juez Patel dictó sentencia ordenando a las compañías discográficas notificar a Napster un listado sobre temas a eliminar del servicio en un plazo de 72 horas. Esta sentencia fue apelada y confirmada por el tribunal de apelaciones.

De todos modos y al margen del fallo, el filtro de temas era vulnerable, ya que luego aparecieron temas con pequeñas modificaciones en sus nombres, por lo que igualmente seguían las descargas no autorizadas sin pagar los derechos de autor.

Todo esto anunciaba, que la solución del caso Napster no generaba una solución a la problemática del fenómeno MP3.

c) Otros sitios similares

Luego de Napster aparecieron sitios renovados y con mejores servicios para los usuarios; uno de ellos fue Audio Galaxy, que poseía una base de datos tan gran-

de, que parecía que no eran sólo los usuarios quienes compartían la música. Este sitio se hizo pago y luego desapareció.

Más tarde aparecieron otros similares a Napster como Kazaa, Grokster, Winmix, etcétera. Todos estos *software* gratis incluso aparecen en páginas tales como download.com, lo que facilita aún más el acceso a ellos y seguirán apareciendo nuevas posibilidades para la transferencia de archivos de música por Internet.

d) Otras opiniones

Hasta aquí hemos considerado el caso "Napster" desde la versión oficial, es decir, desde la bibliografía e información que se produce desde un único interés: el interés de las compañías discográficas. Son ellas las únicas interesadas en que se conozca el caso "Napster" y en que se suprima toda aquella tecnología distinta a la que ellas ofrecen en el mercado.

Un tratamiento objetivo del tema tendría que escuchar también a los usuarios de Napster y otras personas que no sean voceros de las compañías discográficas.

1) Ha dicho Stephen Bradley, miembro de la firma investigadora de mercado Gartner Group que "las compañías disqueras deben ser muy cuidadosas sobre lo que están pidiendo"; "su afán miope de cerrar a Napster les hará casi imposible controlar el intercambio de música *on line*"[23].

2) La empresa Júpiter Communications Inc. ha afirmado que los usuarios de Napster son más propensos a la compra de música que los no-usuarios de Napster. Esto se debe, a que los usuarios de Napster son más entusiastas de la música, y que si bien suelen acopiar una numerosa cantidad de archivos en su PC, casi siempre encuentran en la *web* aquel conjunto musical del cual les gustaría tener toda la colección en sus compactos originales[24].

3) Muy importante es también la opinión del cantante Peter Gabriel, que dijo que la distribución de música en Internet, aunque sea ilegal, ha *aumentado la asistencia a sus conciertos*, lo que le ha generado mayores utilidades de las que recibe, por la venta de sus CDs, de sus productores musicales[25].

4) Es llamativo el obrar de la banda Metallica. A mediados del año 2000 le presentó a la empresa Napster.com una lista con 317.377 nombres de usuarios que habían copiado ilegalmente canciones a través del *software* Napster. Metallica no resolvió el problema, pero además *perdió muchos simpatizantes* con esta maniobra.

5) Pero más importante que la opinión de Peter Gabriel o la reacción adversa con Metallica, es la opinión de los usuarios de Napster y de todas las otras comunidades virtuales, sobre todo en aquellas clases sociales donde la compra del CD no es accesible.

La conducta sostenida de los usuarios en todo el mundo, parece estar discutiendo la legitimidad de la norma de propiedad intelectual, o al menos, la legitimidad de las ganancias de un puñado de personas a costa del resto. Quizás sea mucho

[23] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[24] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.
[25] Ossa Rojas, *El fenómeno del MP3 y el caso Napster*.

más cercano a la realidad, interpretar la conducta de los usuarios de Napster como información correcta que exige una respuesta.

El mensaje de los usuarios dice en voz alta: "estamos aquí, somos millones y queremos un cambio".

e) Un Napster "a la criolla"

El caso Napster se produjo en Estados Unidos de América, a pesar que la revuelta produjo sus efectos en gran parte del mundo. Sin embargo, no está escrito en ningún lugar, que casos como el de Napster tengan que darse exclusivamente en dicho país.

La Argentina posee programadores altamente capacitados. No es fácil de descartar la hipótesis de un Napster "a la criolla". Ahora bien, ¿sería lícita o ilícita la existencia de un Napster "a la criolla"? ¿Hay algún tipo penal que regule la conducta de un Napster "a la criolla"?

Esta hipótesis fue planteada por Vibes y Alesina, quienes consideran que la ley aplicable en tal caso sería la ley 11.723 de propiedad intelectual. Punto central de la argumentación de estos autores, es que el archivo MP3 encuadra en el concepto técnico de "fonograma". Según la definición del glosario OMPI y el art. 3°, inc. b, de la Convención de Roma, "fonograma es toda fijación exclusivamente sonora de los sonidos de una ejecución o de otros sonidos"[26].

La cuestión no es tan simple. En realidad, sería más claro un caso de reproducción de discos compactos. Esto sí encuadraría en la ley 11.723.

Pero el uso de los archivos MP3 presentan muchos matices.

1) El primero, es que mucha gente compra el CD y luego lo comprime en archivo MP3 para usarlo en la computadora, por ejemplo, durante el trabajo de oficina. Con esto se logran dos cosas: salvaguardar el CD original, y por otro lado, no gastar la lectora de CD de la computadora (la lectora de una PC es sensiblemente más débil que la lectora de un aparato de sonido). Esta situación, por su parte, es análoga a la copia de *software* para salvaguarda de los programas de computación (art. 9°, ley 11.723, texto ley 25.036).

Es decir, ante un caso tal, el abogado defensor del usuario del Napster "a la criolla" va a invocar el art. 9 de la ley 11.723 versión ley 25.036 por analogía *in bonan partem*. Aquí tenemos una causa de justificación prevista en una ley especial.

2) Otro de los matices, se refiere a las diferencias entre el formato MP3 y el formato CD (*wab*). "Reproducir un CD y copiarlo en otro CD virgen" no es exactamente lo mismo que "emepetrear" un CD. Al comprimir en archivo MP3 un CD se pierden algunos datos, y esto marca la diferencia entre "reproducir" y "emepetrear". Se puede intentar sostener que "emepetrear" es algo análogo a "reproducir", pero con esto ya se orienta la interpretación en contra del reo. Aquí se manifiesta una vez

[26] Vibes - Alesina, *El caso "Napster" ¿Un fallo paradigmático?*, *LL*, 2001-D-171.

más, la diferencia entre concebir al derecho penal como carta magna del delincuente o como carta magna del ciudadano[27].

3) Al momento de la sanción de la ley 11.723, no existía el formato MP3. Nadie había imaginado un caso tal. Sin embargo, el Congreso aún no tiene una norma penal que reprima la acción de comprimir un CD en MP3.

4) Desde la óptica de la ley 25.156[28], el usuario es la víctima de un abuso de la posición dominante que ejercen las compañías discográficas en una o varias partes del mundo. Entre ellas, al ser el mercado de música únicamente en CD, no hay competencia sustancial. Esto está previsto por los incs. *a* y *b*, del art. 4°, de la ley 25.156.

Y sobre todo, el formato MP3, debido a sus ventajas frente al CD, parece sí ser una competencia sustancial. La conducta generosa por parte de Napster, también puede entenderse como alguien que "está pagando su derecho de piso" y que quiere ser oído por compañías discográficas, que obviamente, no lo van oír sino cuando no les quede otra alternativa. Es una costumbre comercial que, al lanzar un producto, se hagan ciertas promociones.

En general, el precio de los CD suele ser el mismo en el mercado, a pesar de la existencia de distintas compañías. El inc. *a*, del art. 2° de la ley 25.156 prohíbe fijar, concertar o manipular en forma directa o indirecta el precio de venta, o compra de bienes o servicios que se ofrecen o demanden en el mercado, así como intercambiar información con el mismo objeto o efecto.

Por otro lado, la conducta de las compañías discográficas de pretender excluir a Napster del mercado, parece ser también otra práctica restrictiva de la competencia. El inc. *f*, del art. 2°, de la ley 25.156 considera práctica restrictiva "impedir, dificultar u obstaculizar a terceras personas la entrada o permanencia en un mercado o excluirlas de éste". En este sentido parece tener razón el abogado de Napster.

Estos planteos pueden continuar. Con esto sólo queremos demostrar que no es tan simple la punición de un caso Napster "a la criolla". La acción de "emepetrear" requiere un tipo penal autónomo de *lege ferenda*. En este sentido, no se debería confundir los aspectos civiles con los aspectos penales de la ley 11.723.

3. El virus informático

a) Concepto

Preferimos la definición de Kutten, quien define al virus informático, como un programa de computación que puede diseminarse de una computadora a otra sin la intervención de un usuario y sin que éste tenga conciencia de la transmisión. Cada programa infectado, a su vez, infecta a otro. Una vez allí toma el control de la com-

[27] Naucke, *Strafrecht. Eine einführung*, § 2, núm. marg., 29 y ss, p. 68.

[28] Brond, Leonardo G., *Propuesta de modificación al art. 53 de la ley 25.156*, "Revista Aequitas", n° 13, mar.-may., 2003, p. 50 a 53.

putadora[29]. Siguiendo esta definición, surgen las tres características principales del virus informático: *1*) produce un daño; *2*) es autoproductor, y *3*) es subrepticio.

Su funcionamiento es muy sencillo; luego de ser programado por su autor, el virus es insertado en un lugar al que tengan acceso muchas personas (p.ej., una red pública, una base de datos). Allí el programa irá infectando sucesivamente –mediante el proceso de hacer copias de sí mismo– todos los disquetes *o floppy disk* que sean introducidos en esa computadora. Estos disquetes serán llevados a otro ordenador, este ordenador se infectará y el ciclo comenzará de nuevo. Esto dura hasta que el virus sea detectado o produzca sus efectos. El funcionamiento es también, sin embargo, una señal para distinguir entre el virus informático y otros conceptos cercanos que también producen daños. Las categorías son tres[30]:

1) *Caballo de Troya*. Es un programa de apariencia normal, que disfrazado bajo la forma de programas útiles, o en un *e-mail* destruye la información almacenada en la computadora.

2) *Gusano*. Es similar al virus, pero no puede regenerarse. Podría decirse que un gusano es un "tumor benigno" mientras que un virus es un "tumor maligno". A través de un gusano se podría dar instrucciones al sistema informático de un banco para transferir de modo continuo dinero a cuentas ilícitas.

3) *Bomba lógica o cronológica*. Requiere la programación de la destrucción o alteración de datos en un momento dado del futuro. Son difíciles de detectar.

b) Algunos de los virus más famosos

1) *Brain, Scores, Jerusalem*. El virus Brain atacó a los ordenadores compatibles con IBM. En el año 2000, este virus recorría el mundo entero infectando cuanto ordenador encontraba. Llegó a las computadoras del diario *The Providence Journal* de Rhode Island, donde un reportero que estaba escribiendo perdió la nota.

Los técnicos no pudieron recuperar la información en el ordenador, pero en el disco rígido encontraron un número telefónico al que llamaron y se comunicaron con un joven programador paquistaní, Basit Anjad, quien junto con su hermano se reconoció autor del virus y explicó que lo había creado para proteger sus programas[31].

La explicación dada por Basit Anjad puede ser interpretada como una "causa de justificación" similar a las "offendículas"[32].

El virus Scores atacó las computadoras Macintosh de la Universidad de Miami. También afectó a la enorme firma de computación EDS (una subsidiaria de la General Motors), firma que justamente –como uno de sus servicios– garantiza la seguridad de los datos de sus clientes. Por esa razón –para no alegar su propia torpeza– se negaron a admitir la existencia de virus en sus sistemas y no denunciaron el caso[33].

---

[29] Palazzi, Pablo A., *Virus informáticos y responsabilidad penal*, *LL*, 1992-E-1123.
[30] Levene (n.), Ricardo - Chiaravalloti, Alicia, *Delitos informáticos*, *LL*, 1998-E-1234.
[31] Palazzi, Pablo A., *Delitos informáticos*, Bs. As., Ad-Hoc, 2000, p. 147 y 148.
[32] Artificios que el propietario emplea para proteger su dominio.
[33] Palazzi, *Delitos informáticos*, p. 147.

El virus Jerusalem se llama así porque fue descubierto en los ordenadores de la universidad homónima, en diciembre de 1987. Un programador advirtió que su computadora trabajaba más lenta los días 13 de cada mes. Investigando descubrió el virus. El "Jerusalem" estaba preparado para borrar, el viernes 13 de mayo de 1988, las memorias de los ordenadores que infectara.

Afortunadamente faltaban cinco meses, suficientes para prevenir a las víctimas potenciales y buscar el antídoto[34].

2) *Datacrime, Datacrime II y Datacrime IIb*. El virus Datacrime también conocido como el *Columbus Day Virus*, apareció en gran parte del mundo provocando graves daños.

Este virus se activa todos los 12 de octubre, mostrando el siguiente mensaje: "*Datacrime Virus, Released:1 March 1989*" y luego realizaba un formateo de bajo nivel en el disco rígido, destruyendo toda la información que el usuario había almacenado.

El centro del problema fue Europa. En Francia fueron atacadas las empresas Telecom, Thompson, Renault, Maltra, Ferrocarriles de Francia y la Universidad de París. En Holanda resultaron atacadas las empresas Shell, Akzo, Philips y los ferrocarriles holandeses[35].

A medida que el virus se iba haciendo fácil de detectar, fueron apareciendo otras versiones que dificultaban su detectamiento. Así apareció el virus Datacrime II, cuyos efectos destructivos eran similares al Datacrime, pero cuya localización era más dificultosa.

Otro tanto puede decirse respecto del virus Datacrime IIb, que contaba con una técnica de encriptado que impedía ser descubierto hasta muy poco tiempo antes de producir el daño.

3) *I love you*. Este virus –también conocido con el nombre "love bug" fue introducido en la red Internet desde Filipinas y causó importantes daños en sistemas informáticos a nivel mundial. Produjo la paralización de la actividad de varias compañías en todo el mundo, mediante el envío de millones de correos electrónicos, que hicieron colapsar los servidores[36]. Según noticias periodísticas provenientes de Filipinas, el estudiante acusado de lanzar el virus quedaría impune atento a la carencia de leyes que sancionen este delito en Filipinas[37].

4) *Chernobil*. El virus Chernobil, también llamado CIH, fue inventado –como la mayoría de los virus– por un joven entre 17 y 24 años, con inteligencia superior a la media, que pretende que su arte sea reconocido en el mundo informático. Apareció por primera vez en junio de 1998 en Taiwán. Estaba programado para actuar el día del 13° aniversario de la catástrofe de la central nuclear de Chernobil (Ucrania).

Este virus es capaz de dañar la BIOS del ordenador. La BIOS es la parte de la PC encargada de mantener los datos vitales del sistema y ejecutar el arranque del

[34] Palazzi, *Delitos informáticos*, p. 147.
[35] Palazzi, *Delitos informáticos*, p. 148.
[36] Durrieu - Lo Prete, *Delitos informáticos*, *LL*, 2002-A-1287.
[37] Fernández Delpech, Horacio, *Protección jurídica del software, con comentarios de la legislación iberoamericana*, Bs. As., Abeledo-Perrot, 2000, p. 62.

ordenador. Presenta la cualidad de reenviarse por *e-mail*. Es un virus residente en la memoria, que infecta ficheros ejecutables (EXE) de *Windows* 95/98 y se oculta en huecos libres del programa infectado, por lo que el archivo dañado no aumenta de tamaño. La PC no puede volver a funcionar hasta que no se vuelva a grabar la información borrada por el virus.

Se ha dicho también, que el daño que ocasiona es tan grande, que obliga a comprar una nueva placa. Otra alternativa es mandar la placa a la fábrica para que la devuelvan escrita de nuevo, pero esto es más caro que comprar una placa nueva. De allí que esta alternativa esté fuera del alcance de la mayoría de los usuarios cibernéticos. En cuanto a la cualidad del daño, está considerado por expertos como un virus destructivo de *hardware*, ya que la BIOS está considerada como parte del *hardware*[38]. Los daños causados por el CIH, a diferencia de otros virus, no se solucionan reinstalando todos los programas.

Existen tres versiones de este virus, que se diferencian en la fecha en la que llevan a cabo su acción dañina (*payload*). El CIH versión 1.2 se activa el 26 de abril; la versión 1.3, el 26 de junio, y la 1.4 el 26 de cada mes. La primera versión, la 1.2 es la más conocida, porque lleva consigo el alias de Chernobil.

No hay unanimidad entre los expertos sobre el alcance real de los daños causados por este virus, porque su cuantificación es complicada y relativa a cada país. Algunos lo caracterizan como uno de los más destructivos de los últimos tiempos. Otros lo consideran como puramente anecdótico, sobre todo en Europa y Estados Unidos de América.

La empresa finlandesa Data Fellows señaló que los mayores daños del virus tuvieron lugar en Asia, Medio Oriente y ciertos países europeos, donde los programas piratas son de uso cotidiano. España se incluye en este grupo.

El gobierno de Corea del Sur afirma que alrededor de 300.000 PCs fueron infectadas, aproximadamente un 4% del total, los mismos datos que en Turquía. Fuentes de los Emiratos Árabes aseguran que en su caso, cerca de un 10% de la base total de los ordenadores han sido dañados. En la India y Bangladesh los perjuicios son similares, así como en China. De ser ciertos estos datos, los daños se traducirían en miles de millones de dólares de pérdidas en estos países. Según los expertos asiáticos, se hizo caso omiso de las múltiples advertencias.

En Estados Unidos de América, por el contrario, el efecto del virus Chernobil fue considerablemente menor. Los norteamericanos se lo han tomado mucho más en serio, sobre todo en los entornos operativos. De esta manera, son principalmente los usuarios domésticos, los que han acusado la acción de este virus.

c) El caso “Pinamonti” (relacionado con el “caso de la computadora”)

1) El caso “Pinamonti”[39] es un fallo muy importante en materia de daño informático. Las circunstancias de hecho de este caso eran las siguientes: ante la ruptura de una relación contractual, un programador reclamó a la empresa contratante la

[38] Para mayor información consultar: http://www.hispasec.com; http://www.pandasoftware.es, etcétera.

[39] CNCrimCorr, Sala 6, 30/4/93, “Pinamonti, Orlando M.”, *JA*, 1995-III-236.

devolución del *software* que había entregado. Frente a la negativa de la empresa, se inició una denuncia por el delito de retención indebida. No siendo posible probar tal retención, y con la certeza de que el *software* había sido borrado del ordenador de la empresa querellada, se argumentó que la eliminación de un programa de computación almacenado en un soporte magnético constituye el delito de daño.

2) Los problemas de aplicación de la ley, que presenta el caso "Pinamonti" son muy similares a otros problemas mencionados en la literatura jurídico-penal, como por ejemplo "el caso de la computadora".

Las circunstancias de hecho del "caso de la computadora"[40] son las siguientes: en una central de procesamiento de datos de una gran empresa, un empleado por enojo sobre el mal clima de la empresa, interrumpe el suministro de energía para la computadora en un lugar difícil de descubrir, sin dañar las conexiones mismas; la central no puede trabajar durante varias horas. En el "caso de la computadora" se discute, entre otras cosas, si se trata del delito de daño (§ 303, StGB), o de alteración de datos (§ 303a, StGB).

A continuación veremos la decisión judicial del caso "Pinamonti" y veremos también las voces que se alzaron en su contra. Anticipamos desde ya, que no es posible la punición de la alteración de datos, debido a la falta de un precepto penal preciso específico.

1) *La decisión judicial del caso "Pinamonti"*. La Cámara resolvió que: *1*) El *software* es una obra intelectual en los términos de la ley 11.723; *2*) la ley de derecho de autor no contempla en las acciones típicas de sus delitos el borrado o destrucción de programas de computación (arts. 71 a 73, ley 11.723), y *3*) el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño, pues el concepto de cosa es aplicable al soporte y no a su contenido (art. 183, Cód. Penal).

El tribunal confirmó el auto, aun cuando sobreseyó definitivamente en la causa, en la que no se procesó a persona alguna. El fallo tiene la firma de los camaristas Elbert y Camiña.

2) *La interpretación de Palazzi*. Este autor ha criticado el fallo argumentando que el borrado o destrucción de un borrado de computación es punible tanto de *lege lata* como de *lege ferenda*. En concreto, Palazzi propone cuatro soluciones:

a) Una interpretación amplia del concepto de "cosa" del art. 183 del Cód. Penal. Esta tesis no tiene ningún argumento, sino que se limita a considerar la jurisprudencia –también discutible– que incluía a la electricidad dentro del concepto de cosa aun antes de la reforma de 1968, como así también, la jurisprudencia referida a las imágenes de televisión y a los pulsos telefónicos[41].

Una debilidad de esta tesis radica en extender el concepto de "energía eléctrica" al concepto de "energía magnética". Tal concepto de "energía magnética"[42] es casi un argumento *ad hoc*.

---

[40] Naucke, *Strafrecht. Eine einführung*, § 1, núm. marg. 116, p. 28.

[41] Palazzi, Pablo A., *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-238.

[42] Palazzi, *Virus informáticos y responsabilidad penal*, *LL*, 1992-E-1127.

Esta tesis tiene en contra además, el principio de la interpretación estricta de la norma penal. No estamos de acuerdo con esta opinión.

b) Observa Palazzi, que el fallo en cuestión distinguió entre continente –el soporte– como cosa en los términos del art. 183 y contenido –el *software* o los datos–. Palazzi propone considerar al *software* como lo principal y al soporte como lo accesorio.

El problema de esta tesis radica, en que hay que salir del tipo penal, recorrer algunas normas del Código Civil, formular consideraciones jurídicas en base al derecho civil y luego aplicar esa interpretación en el tipo penal en contra del imputado.

Esto también es una interpretación amplia del concepto de cosa, aunque no esté planteada así. Tampoco estamos de acuerdo con esta tesis de Palazzi.

c) La tercera posibilidad, ya no se refiere al objeto "cosa" sino a considerar la afectación de la función de la cosa y su valor económico. Si la acción realizada, sostiene Palazzi, afecta la función que cumple el objeto o su valor económico, se produce un daño conforme al art. 183 del Cód. Penal.

La acción de daño, dice Palazzi –citando a Creus– está constituida por todo ataque a la materialidad, utilidad o disponibilidad de las cosas, que elimine o disminuya su valor de uso o cambio. La utilidad se ataca cuando se elimina la aptitud que la cosa tenía para el fin que estaba destinada o se disminuye tal aptitud[43].

Los ejemplos son numerosos: el valor de la cinta de un *cassette* con una sinfonía de Mozart no es el mismo, que el valor de la cinta borrada[44]; el valor de una cinta de un *cassette* donde Pedro tenía grabada conversaciones con su novia María, tampoco es el mismo[45].

d) La cuarta solución ofrecida por Palazzi consiste en modificar el Código Penal para reprimir esta clase de delitos. Estamos de acuerdo con ello.

3) *La interpretación de Fernández Delpech*. Otra voz que se suma a la opinión de Palazzi, es la de Fernández Delpech. Para este autor, el borrado o destrucción de programas o introducción de virus informáticos debería ser punible conforme al art. 183 del Cód. Penal. En verdad, coincide con Palazzi en muchos puntos, además de no proponer argumentos nuevos. Salvo este: "La información contenida en un ordenador tiene la forma de energía"[46].

4) *Nuestra interpretación*. Consideramos que la decisión de la Cámara Criminal en el caso "Pinamonti" es correcta. Teniendo en cuenta lo vinculado que se encuentran los jueces penales al decidir (tipicidad y prohibición de analogía) y las lagunas normativas existentes en el tema, las soluciones no pueden provenir de los órganos jurisdiccionales sino del legislador.

[43] Creus, Carlos, *Derecho penal. Parte especial*, t. 1, 6ª ed., Bs. As., Astrea, 2002, p. 573.
[44] Pellicori, Oscar A., *Informática y delito*, *ED*, 157-859.
[45] Naucke, *Strafrecht. Eine einführung*, § 1, 107, el "caso de la cinta", p. 26.
[46] Fernández Delpech, *Internet: su problemática jurídica*, p. 166.

Hay consenso en que es difícil de establecer los límites entre interpretación de la ley y aplicación por analogía[47]. A nuestro criterio, si en el caso "Pinamonti" se hubieran aplicado penas por el delito en una cosa inmaterial, se hubiera aplicado la ley por analogía.

Si bien se distingue entre analogía *in malam partem* y analogía *in bonam partem*, consideramos que la aplicación de una pena al daño inmaterial (los datos y programas) sería una analogía *in malam partem*, fundada en el daño material (la cosa). Y es precisamente la analogía *in malam partem* la que está prohibida (art. 18, Const. nacional)[48]. El derecho penal es un sistema discontinuo de ilicitudes y existen lagunas que no tienen que ser llenadas[49].

Los intentos de punir la introducción de un virus (alteración de datos) sin una ley expresa se acercan también al invento de un profesor de la Universidad de Montevideo, en 1933, que consistía en el "delito innominado". Para la configuración del "delito innominado", el profesor Salvagno Campos exigía los siguientes requisitos: *1*) la violación de una norma o de un interés jurídico individual consagrado del modo que sea en la ley punitiva, y *2*) carácter eminentemente injusto de la conducta por la ausencia de todo derecho legal o natural que hubiera podido favorecer al autor[50].

Opinamos que la tercera posibilidad manifestada por Palazzi es convincente, pero es una consideración que está mucho más cerca del delito de "alteración de datos", que del delito de daño.

El delito de daño en el Código Penal alemán (§ 303, StGB) tiene un contenido equivalente al art. 183 del Cód. Penal argentino. En el delito de alteración de datos en el Código Penal alemán, no tiene un equivalente típico en el Código Penal argentino. De allí las interpretaciones forzadas –inconstitucionales– sobre el art. 183 del Cód. Penal argentino, o las propuestas de modificación a nuestro Código Penal.

En general, los autores argentinos que escriben sobre derecho informático coinciden en la necesidad de punir lo que en Alemania se llama alteración de datos (§ 303a, StGB) y que en Argentina se designa en base al concepto de cosa –art. 2311, Cód. Civil– como "cosas intangibles".

Es que hablar de un delito de daño sin producir un daño efectivo en la cosa, resulta ser contradictorio. Es mucho más claro un precepto penal específico que se refiera directamente a la alteración de datos. Esto también es conforme a las exigencias constitucionales de la punibilidad.

---

[47] Schmidhäser, *Lehrbuch*, p. 112, citado por Bacigalupo, Enrique, *Manual de derecho penal. Parte general*, Bogotá, Temis, 1998.

[48] Núñez, Ricardo C., *Manual de derecho penal. Parte general*, 4ª ed., Córdoba, Lerner, 1999, p. 68 y 69; Creus, Carlos, *Derecho penal. Parte general*, 5ª ed., Bs. As., Astrea, 2003, p. 61; Muñoz Conde, Francisco - García Arán, Mercedes, *Derecho penal. Parte general*, 3ª ed., Valencia, Tirant Lo Blanch, 1998, p. 133; Soler, Sebastián, *Derecho penal argentino*, t. IV, 4ª ed., Bs. As., Tea, 2000, p. 541 ss.; Fontán Balestra, Carlos, *Derecho penal. Parte especial*, 16ª ed., Bs. As., Abeledo-Perrot, 2002, p. 595 ss y en especial: p. 191 y 383 en relación a la ley 25.326 de 2000, que incorporó los arts. 117 *bis* y 157 *bis* al Código Penal.

[49] Nino, Carlos S., *Introducción al análisis del derecho*, 2ª ed., Bs. As., Astrea, 2003, p. 285.

[50] Jiménez de Asúa, Luis, *La ley y el delito. Principios de derecho penal*, Bs. As., Sudamericana, 1967, p. 126.

Por ello, no podemos coincidir con Palazzi. Sólo es posible punir la alteración de datos (o cosas inmateriales, como dice Palazzi), luego de crear los preceptos penales correspondientes.

El argumento de Fernández Delpech "la información contenida en un ordenador tiene la forma de energía" es muy vago, y está encaminado a extender el concepto de energía eléctrica a lo que Palazzi denomina "energía magnética".

Hemos manifestado estar en desacuerdo con aquella opinión de Palazzi. En consecuencia, también estamos en desacuerdo con esta extraña argumentación.

La modificación de la ley para incluir el delito de "alteración de datos" no está tan lejos como parece, en noviembre de 2000, fue sancionada la ley 25.326. Esta ley incorpora al Código Penal los arts. 117 *bis* y 157 *bis*.

El tipo penal del art. 117 *bis* contempla la conducta de "el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales" (inc. 1°); "al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales" (inc. 2°); habiendo agravantes si de tal información falsa resulta perjuicio a alguna persona (inc. 3°), y si el autor o responsable fuese un funcionario público en ejercicio de sus funciones (inc. 4°). El tipo penal del art. 157 *bis* reprime al que "a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".

Si bien se considera que hay mala técnica legislativa, y que la ubicación del tipo penal en el art. 117 *bis* dentro de los "delitos contra el honor" es desafortunada[51], cabe mencionar esta reforma como indicio de una reforma futura más precisa y más abarcativa, y que contemple expresamente, la introducción de un virus informático destructivo del *software*.

d) ¿Es delito la activación de un virus informático?

Esta pregunta se ha tornado de muy difícil respuesta en los últimos tiempos. Una parte de tales dificultades son las que presenta el tema por sí mismo. Pero otra parte de las dificultades las trae la doctrina de los juristas.

Hay una idea entre muchos juristas, de que el virus no daña la computadora sino que daña los datos que contiene, y que los datos son un objeto inmaterial.

Fernández Delpech, por ejemplo, dice que: "estas conductas, que consisten en el borrado o destrucción de programas o en la introducción de virus mediante cualquiera de sus formas, el objeto dañado no es la computadora (cosa mueble), sino que *lo que daña es la información que ella posee*, y que como tal es un objeto inmaterial de difícil caracterización"[52].

Los jueces del caso "Pinamonti" dieron por sentado, que el virus ataca a los programas y a la información, de allí la decisión tan criticada.

---

[51] Fontán Balestra, *Derecho penal. Parte especial*, p. 191 y 383.

[52] Fernández Delpech, Horacio, *Protección jurídica del software, con comentarios de la legislación iberoamericana*, Bs. As., Abeledo-Perrot, 2000, p. 59.

La decisión de que "el concepto de cosa es aplicable al soporte y no a su contenido" presupone necesariamente que el virus ataca al contenido, es decir, a los programas y a la información.

Palazzi en sus trabajos a favor de la punición del virus como delito de daño, parte de que el virus afecta a la información y a los programas[53].

Más concretamente, "el virus informático produce un daño borrando la información contenida en la computadora. Es importante aclarar que no es la computadora en sí misma el objeto dañado, sino la información que ésta posee"[54].

Aclaramos que los virus que atacan la computadora producen el delito de daño en el sentido tradicional del término, porque atacan una cosa (material). Remitimos a los desarrollos e interpretaciones de los autores de la parte especial del derecho penal, por considerar suficiente el hecho de demostrar la existencia de virus que destruyen la computadora[55].

El problema se plantea con la otra clase de virus, a saber, con los virus tradicionales que sólo destruyen los programas y los datos, pero que no destruyen la computadora. Esto requiere gran atención, y vamos a desarrollar el tipo objetivo y el tipo subjetivo del delito de daño, según las tesis que sostienen de *lege lata* la punibilidad del daño en base al art. 183 del Cód. Penal. Dejamos aclarado que no compartimos el criterio expuesto a continuación como tipo objetivo y subjetivo.

1) *Tipo objetivo*. Se sostiene que el delito de introducción de virus en una computadora se encuentra alcanzado por el art. 183 del Cód. Penal, a pesar de no estar expresamente legislado. La acción consistiría en contaminar una computadora, ya sea a través de una línea telefónica por un MODEM (*modulation demodulation*) o insertando directamente un disquete a sabiendas de que está infectado[56].

Aquí entra en juego nuevamente el concepto de "energía magnética", que ya hemos criticado.

Palazzi intenta apoyarse también en la expresión "cualquier modo" prevista en el art. 183 del Cód. Penal[57].

Un fallo que tiene mucho peso en la argumentación de Palazzi es el caso "Oliva", donde la Cámara argumentó que "el delito de daño no exige que la cosa mueble o inmueble quede totalmente destruida o inutilizada: basta para su consumación que la restitución del bien a su estado anterior demande algún gasto, esfuerzo o trabajo"[58].

A mayor abundamiento, Palazzi intenta hacer entrar en juego el tipo de daño agravado previsto en el inc. 5°, del art. 184, del Cód. Penal, referido a archivos, registros, bibliotecas o museos públicos. El argumento expresa que el archivo o regis-

[53] Palazzi, Pablo A., *Delitos informáticos*, Bs. As., Ad-Hoc, 2000, p. 133 a 157.
[54] Palazzi, *Virus informáticos y responsabilidad penal*, *LL*, 1992-E-1127.
[55] Núñez, *Manual de derecho penal. Parte especial*, p. 267 ss; Breglia Arias, Omar - Gauna, Omar R., *Código Penal y leyes complementarias, comentado, anotado y concordado*, t. 2, 4ª ed., Bs. As., Astrea, 2001, p. 344 y siguientes.
[56] Palazzi, *Delitos informáticos*, p. 150.
[57] Palazzi, *Virus informáticos y responsabilidad penal*, *LL*, 1992-E-1128.
[58] CNCrimCorr, Sala IV, 13/2/90, "Oliva, Jorge J.", *LL*, 1990-C-265; *ED*, 138-722.

tro electrónico quedaría comprendido, ya que no hay diferencias en cuanto al soporte; una biblioteca es *asimilable* a un banco de datos informatizado.

Pero es esta palabra "asimilable" (posible de asimilar) la que demuestra la notoria intención de aplicar la ley penal por analogía. Pese a toda esta argumentación, seguimos sosteniendo que la introducción de un virus en una computadora es una conducta atípica en el derecho penal argentino vigente; es decir, que esta tesis de Palazzi es una interpretación forzada de la ley[59].

2) *Tipo subjetivo*. El tipo subjetivo requiere, según Palazzi, no sólo el conocimiento del carácter dañino del programa (no se requiere que sea específico, referido a la forma de dañar) sino también el conocimiento y voluntad de que causará esos efectos en ese ordenador. El dolo podrá ser eventual si el autor no sabe cuándo se activará el virus, en el caso de ser una bomba lógica. No existe daño culposo.

Para nosotros este tema no entra en cuestión, dado que no resultó convincente la argumentación a favor de la tipicidad objetiva de *lege lata*.

e) La activación de un virus "de lege ferenda"

Varias son las opiniones que consideran, que recién en caso de modificar la ley será posible la punición de la alteración de datos. Aquí ofrecemos las opiniones de algunos autores y legisladores. Además de ser ésta, nuestra opinión.

El acuerdo sobre la necesidad de reformar la ley se agota allí. A la pregunta acerca de cómo sería la reforma del Código, cada autor tiene su propio proyecto. Por eso reproducimos aquí las siete tesis más difundidas.

1) *La tesis de Palazzi*. Conforme a esta opinión, habría que reformar el artículo de daño, para que incluya de alguna manera amplia el daño sobre los datos en un sistema informático. Ello podría alcanzarse incluyendo el término "intangible" a la lista de elementos pasibles de daño. La redacción reformada sería:

"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 *o intangible*, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

La reforma abarcaría también la definición del término "intangible" y su incorporación al art. 77 del Cód. Penal[60].

2) *El proyecto de Leonor Tolomeo*. Este proyecto denominado "ley contra los delitos informáticos"[61] es más abarcativo, dado que propone modificar los arts. 77, 153, 157, 173 incs. 1°, 2°, 8°, 12; 175, 183, 184 inc. 5°, 186 inc. 3°, 194, 197, 222, 255; incorporar un segundo párrafo del art. 154. La palabra *software* está incluida en todos estos artículos. Ejemplo del art. 173: "El que cometiera defraudación, sustituyendo, ocultando o mutilando algún proceso, expediente, documento, otro papel importante o *software*.

[59] De acuerdo: Durrieu - Lo Prete, *Delitos informáticos*, *LL*, 2002-A-1287.
[60] Palazzi, *Delitos informáticos*, p. 157.
[61] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1237.

Con respecto al delito de daño, el art. 183 quedaría redactado de la siguiente manera: "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 *o un software de forma tal que fuere parcial o totalmente irrecuperable*, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. Si el *software* fuere recuperable totalmente por la existencia de copia de seguridad actualizada, la pena se reducirá de un tercio a la mitad".

Respecto al art. 77, la reforma incluiría definiciones tales como: *software*, *software* de datos, *hardware*, soporte electrónico y sistema informático.

3) *El proyecto de Carlos Álvarez*. Este proyecto contiene tres artículos, estableciendo pena privativa de libertad y pena de multa. Los tipos penales son: "el que se apropiare de datos o informaciones reservadas o representativas de bienes o derechos" (art. 1°); "el que a sabiendas y sin autorización, usare, alterare o dañare una computadora, sistema o red informática, cualquier soporte lógico, programa o documentación de la computadora o datos contenidos en la misma" (art. 2°).

El art. 2° agrava la pena si la destrucción de una computadora, sistema o red informática es definitiva.

El art. 3° reprime a quien "mediante el uso o la utilización de una computadora o una red informática defraudare a otro"[62].

A nuestro criterio este proyecto confunde mucho los conceptos.

4) *El proyecto de José Romero Feris*. Este proyecto contiene cinco artículos y es muy parecido al proyecto de Carlos Álvarez.

Merece destacarse la existencia de un agravante para los funcionarios públicos: inhabilitación especial perpetua[63].

Este proyecto es pasible de las mismas críticas del anterior.

5) *El proyecto de Antonio Berongaray*. Este proyecto se parece a las leyes alemanas, por lo menos, eso sugiere la extensión de su nombre: "Reglamentando las actividades vinculadas a computadoras, sistemas de computación o telecomunicaciones".

El proyecto contiene 9 capítulos, cuyos títulos son: "Glosario de términos: computadora, sistema de computación, datos, programas de computación, función de interceptar" (cap. 1); "Del acceso no autorizado" (cap. 2); "Daño a datos informáticos (cap. 3); "Violaciones a la propiedad intelectual en materia de programas de computación no comprendidas en la legislación específica" (cap. 4); "Fraude por medios informáticos" (cap. 5); "Espionaje a través de la computación" (cap. 6); "Entrega, distribución y venta de medios destinados a cometer delitos previstos en este capítulo" (cap. 7); "Normas procesales" (cap. 8); "Disposiciones transitorias y complementarias" (cap. 9)[64].

[62] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1239.
[63] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1239.
[64] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1239.

6) *El proyecto Quinzio, Adunez, Figueroa y Galván*. En este proyecto se propone la incorporación de un art. 183 *bis* al Cód. Penal, con el texto siguiente:

"Será reprimido con prisión de un mes a tres años, el que destruyere, borrare, inutilizare, o de cualquier modo dañare los *datos o programas* total o parcialmente ajenos contenidos en soportes magnéticos, electrónicos, o en sistemas o redes informáticos, siempre que el hecho no constituya otro delito más severamente penado".

Este es el criterio preferible. Es decir, un artículo aparte, que no esté muy lejos del delito de daño, y en lo posible sólo un artículo que regule esta conducta. Este sistema es además, bastante parecido al sistema alemán y el que se impone en otros países. Este proyecto, por su parte, es más conforme al significado cultural de la codificación[65].

7) *El proyecto publicado en el Boletín Oficial*. Este proyecto, publicado el 26/11/01, es muy abarcativo y fue presentado como una ley especial. Allí se regulan muchas conductas. Con respecto al virus informático, el art. 2° establece: "Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un *sistema o dato informático*".

Durrieu y Lo Prete consideran que debiera incluirse el *entorpecimiento del normal funcionamiento de un sistema informático*[66].

f) El Código Contravencional de la Ciudad de Buenos Aires

Es de destacar que el Código Contravencional de la Ciudad de Buenos Aires contempla parcialmente el tema objeto de este trabajo.

Entre las contravenciones allí descriptas, se encuentra en el art. 44 la acción de "afectar el funcionamiento de los servicios de alumbrado, limpieza, gas, electricidad, agua, teléfono, *transmisión de datos*".

En opinión de Fernández Delpech, toda acción que tienda a afectar el funcionamiento de la transmisión de datos en la ciudad de Buenos Aires debe considerarse al menos una contravención sancionada conforme al art. 50 del mencionado Código Contravencional. Es decir: cualquier acción que afecte la transmisión de datos vía Internet (páginas *web*, *e-mail*, etc.) configura esta contravención[67].

g) Derecho comparado

1) *Advertencia preliminar*. Es muy tradicional, que los autores sobre delitos informáticos complementen sus obras con legislación comparada. La cantidad de normas que puede entrar en juego es inmensa.

---

[65] Soler, Sebastián, *El llamado derecho penal económico*, p. 36, citado por Righi, Esteban, *Los delitos económicos*, Bs. As., Ad-Hoc, 2000; Durrieu - Lo Prete, *Delitos informáticos*, *LL*, 2002-A-1288.

[66] Durrieu - Lo Prete, *Delitos informáticos*, *LL*, 2002-A-1286.

[67] Fernández Delpech, *Protección jurídica del software, con comentarios de la legislación iberoamericana*, p. 62.

El panorama generalmente suele omitir la situación latinoamericana. Así, Palazzi[68] menciona legislación de Estados Unidos de América, Gran Bretaña, Alemania, Austria, Francia, Portugal, Italia y Chile[69]. Levene y Chiaravalloti señalan legislación de Alemania, Austria, Francia y Estados Unidos de América[70]. Fernández Delpech[71] menciona legislación latinoamericana, pero en relación al derecho de propiedad intelectual (no en relación al virus).

Para compensar este menosprecio por la legislación latinoamericana, hemos buscado una gran cantidad de códigos penales y encontramos legislación que nada tiene que envidiarle a los países europeos. Nos referimos al Código Penal boliviano.

La búsqueda se centró en dos normas: *a*) el tipo penal de daño, que existe en todas las legislaciones, y *b*) un tipo penal que pueda abarcar la introducción de un virus que destruya datos. Este tipo no está en todas las legislaciones.

2) *Alemania*. El Código Penal alemán, como ya lo anticipamos, contiene dos preceptos, a saber:

§ 303 (Daño material) I. Quien dañe o destruya ilícitamente una *cosa* ajena será castigado con pena de privación de libertad de hasta dos años o con multa. II. La tentativa será punible[72].

§ 303a (Alteración de datos) I. Quien borre, elimine, inutilice o altere ilícitamente *datos* (§ 202a, ap. II) será castigado con pena de privación de libertad de hasta dos años, o con multa. La tentativa será punible.

§ 202a II. Datos, a efectos del apartado I, serán sólo aquellos que no sean almacenados, transmitidos electrónica, magnéticamente, o de forma inmediatamente accesible.

Los comentaristas alemanes suelen explicar al § 303a (Alteración de datos) como *complemento* del § 303 (Daño material). El autor del delito de alteración de datos tiene que ser una persona distinta de la víctima. La acción puede consistir en una comisión o en una omisión. Cuando se alteran varios datos al mismo tiempo, hay concurso ideal, no concurso real. La persecución de este delito se realiza por denuncia del afectado en la generalidad de los casos[73].

Estos tipos penales, junto con otros más, están vigentes desde el 1° de agosto de 1986, cuando se adoptó la 2° ley contra la criminalidad económica.

---

[68] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-240-242.

[69] Palazzi, *Delitos informáticos*, p. 157. Esta simplificación en el derecho comparado conduce a una afirmación errónea.

[70] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1235.

[71] Fernández Delpech, *Protección jurídica del software, con comentarios de la legislación iberoamericana*, p. 69 a 177.

[72] Las traducciones españolas de estos tipos penales están tomadas de la obra: Eiranova Encimas, Emilio (coord.), *Código Penal Alemán StGB. Código Procesal Penal Alemán StPO*, tr. J. Ortiz de Noriega - C. Larios Sánchez - J. C. Peg Ros - A. Monreal Diaz, Barcelona, Marcial Pons, 2000, p. 125 y 164.

[73] Schönke, Adorf - Schröder, Horst, *Strafgesetzbuch. Kommentar*, 25ª ed., München, Beck, 1997, p. 2079 y 2080.

3) *España*. El Código Penal español tiene un sistema parecido al sistema alemán. Contiene un precepto sobre daño y un precepto referido al daño agravado, con un inciso referido a la alteración de datos. Los textos son los siguientes:

Art. 263. "El que causare *daños en propiedad* ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas a la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas".

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".

4) *Bolivia*. El Código Penal boliviano tiene el Capítulo VIII referido a los daños y el Capítulo XI que lleva el título "Delitos informáticos". Las normas son las siguientes:

Art. 357 (Daño simple). "El que de cualquier modo deteriorare, destruyere, inutilizare, hiciere desaparecer o dañare *cosa* ajena, incurrirá en la pena de reclusión de un mes a un año y multa hasta de sesenta días".

Art. 363 *bis* (Manipulación informática). "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días".

Art. 363 *ter* (Alteración, acceso, y uso indebido de datos informáticos). "El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, *datos* almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días".

5) *Uruguay*. El Código Penal de Uruguay sólo contiene el delito de daño expresamente previsto en la ley. Argentina y Uruguay se encuentran en la misma situación. El texto legal es el siguiente:

Art. 358 (Daño). "El que destruyere, deteriorare o de cualquier manera inutilizare en todo o en parte alguna *cosa* mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave con multa de 20 U.R. (veinte unidades reajustables) a 900 U.R. (novecientas unidades reajustables)".

6) *Brasil*. El Código Penal de Brasil contiene el delito de daño en el Capítulo IV, mas no contiene una regulación expresa de un tipo penal referido a la alteración de datos[74]. El texto es el siguiente:

[74] Pero desde el año 1990 hay varios proyectos para tipificar la destrucción de programas o datos almacenados en computadoras [ver Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-242].

Art. 163. "*Destruir, inutilizar ou deteriorar coisa alheia: pena-detenção, de 1 (um) a 6 (seis) meses, ou multa*"[75].

7) *México*. El Código Penal de México regula el delito de daño en el Capítulo X, pero no contiene una regulación expresa de la alteración de datos. El texto es el siguiente:

Art. 161: "Al que por cualquier medio destruya o deteriore una *cosa* ajena o propia, con perjuicio de otro, se le impondrá prisión de seis meses a seis años y de quince a doscientos cuarenta días de multa".

8) *Venezuela*. El Código Penal de Venezuela contiene el delito de daño regulado en el art. 475, pero no hay allí ninguna regulación expresa referida a la introducción de un virus que altere los datos de una computadora.

Art. 475. "El que de cualquier manera haya destruido, aniquilado, dañado o deteriorado las *cosas*, muebles o inmuebles, que pertenezcan a otro, será castigado, a instancia de parte agraviada, con prisión de uno a tres meses".

9) *Chile*. El Código Penal de Chile contiene regulado el delito de daño, y la ley 19.223 tipificó figuras relativas a la informática. El art. 1° se refiere a la destrucción, inutilización, obstaculización o modificación del funcionamiento de un sistema informático.

El art. 3° establece: "el que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor según su grado medio".

Se considera agravante, que el autor esté a cargo de la red o del centro de cómputos. De esta manera queda claro, que Bolivia y Chile son los primeros países de Latinoamérica en contemplar la alteración de datos. La afirmación de Palazzi[76], de que Chile es "el único país de la región que ha actualizado su Código Penal contemplando delitos informáticos", es falsa ya que Bolivia y Chile son los dos países más actualizados en el tema.

10) *Austria*. El Código Penal de Austria contempla el delito de daño y el delito de destrucción de datos. Los datos comprendidos son los personales y no personales (§ 126a, östStGB). Los programas también se encuentran contemplados. Está prevista una pena privativa de libertad de hasta seis meses. La multa, prevista en chelines, ahora debe cotizarse en euros. A medida que aumenta el monto del daño aumenta el monto de la pena privativa de libertad.

Este delito de destrucción de *datos* fue introducido mediante la ley de reforma del Código Penal, del 22 de diciembre de 1987.

11) *Francia*. El Código Penal de Francia contempla el delito de daño y el delito de destrucción de datos. Este último tipo penal, previsto en el art. 462-4 regula la conducta de quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos que éste contiene o los modos de tratamiento o de transmisión.

---

[75] Destruir, inutilizar o deteriorar una *cosa* ajena: pena privativa de libertad de uno (1) a seis (6) meses o multa.

[76] Palazzi, *Delitos informáticos*, p. 157.

La pena prevista es prisión de tres meses a tres años y multa de 2.000 a 500.000 francos.

Este delito fue introducido por la ley 88-19, del 5 de enero de 1988[77], y fue trasladado al art. 323-1 del *Nouveau Code Pénal*: ahora se penaliza a quien al acceder a un ordenador de manera fraudulenta suprime o modifica los datos allí almacenados[78].

El texto del art. 323-1 expresa: "*Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le systéme, la peine est de deux ans d'emprisonnement et de 200.000 Francs d'amende*".

12) *Estados Unidos de América*. Se ha regulado el tema en 1994, en el Acta Federal de Abuso Computacional. Establece multas y prisión de un año para quienes de manera temeraria lancen ataques de virus. Si el virus es lanzado dolosamente, la sanción es multa y diez años de prisión. Esta ley regula los virus informáticos (*computer contaminant*) y se refiere a la contaminación de *programas, grupos de programas y bases de datos*[79].

Sin embargo, parte de estos delitos ya estaban regulados en la ley federal de delitos informáticos (*Computer Fraud and Abuse Act*) de 1986, que contempla en la Sección a 5 la alteración, daño o destrucción de información.

La mayoría de los códigos penales estaduales, salvo el del Estado de Vermont, han tipificado delitos informáticos. Así, el Código Penal de California, en su Sección 502 se refiere a "cualquier persona que maliciosamente... dañe o destruya un *sistema de computación, una red de computadores, un programa de computación o datos* allí contenidos". El Código Penal de Texas determina en su art. 33.03, que será culpable de una ofensa la persona que intencionalmente y con conocimiento y sin autorización del dueño del computador o de la persona autorizada a dar el acceso: *1*) dañe, altere o destruya un computador, o programa de computación o *software*, un sistema informático, datos o una red de computadores[80].

13) *Italia*. El Código Penal italiano tiene previsto el delito de daño y a través de la ley 547, del 23 de diciembre de 1993, está regulado el delito de destrucción de datos. El art. 392 del Código italiano reformado 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*[81].

14) *Portugal*. El Código Penal de Portugal actualmente contempla el delito de daño y el delito de alteración de datos. La alteración de datos fue introducida en 1991, por la ley 109 de delitos informáticos.

El art. 5° de la ley 109, bajo el título "Daño relativo a datos o programas informáticos" establece: "Quien sin estar autorizado, y actuando con la intención de cau-

[77] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1235.
[78] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-241.
[79] Levene (n.) - Chiaravalloti, *Delitos informáticos*, *LL*, 1998-E-1235.
[80] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-241.
[81] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-242.

sar perjuicio a otros u obtener un beneficio ilegítimo para sí o para terceros, extinga, destruya en todo o en parte, dañe, suprima o torne inutilizable *datos o programas informáticos* ajenos o, por cualquier forma, afectare su capacidad de uso, será penado con pena de prisión de hasta 3 años o pena de multa"[82].

15) *Gran Bretaña*. Se han aplicado las leyes comunes (*Criminal Damage Act* de 1971) a la destrucción de datos y programas de ordenador.

La sección 1 (1) de esta ley dispone que "una persona que sin excusa legal destruye o daña cualquier clase de propiedad que pertenezca a otro o que intenta destruirla o dañarla con dolo, o con negligencia acerca de las consecuencias".

El 29 de junio de 1990, se sancionó una ley específica (*Computer Crime Act*), cuya sección 3 contempla la modificación de *datos* como delito (*unauthorised modification of computer material*)[83].

4. Conclusiones

a) Sobre el fenómeno MP3 y el caso "Napster"

1) *Punto de partida de una crisis*. El caso Napster es el *punto de partida de una crisis* de la ciencia jurídica. Generó polémicas y conclusiones, pero no generó soluciones a la problemática planteada. La solución jurídica al caso "Napster" no generó una solución a la problemática del fenómeno MP3.

2) *Quien goza las ventajas, carga con las taras.* El caso Napster hace reflotar la idea de que la compañía discográfica –como cualquier otro sujeto– debe cargar tanto con las ventajas como con las desventajas de la tecnología. Por ejemplo, con la aparición del CD, la empresa discográfica hizo muchas promesas: "el CD suena mejor"; "dura toda la vida", etcétera. En esa época fue cuando el consumidor pasó a pagar casi el doble de lo que costaba un disco o un *cassette*. Aquí la discográfica aprovechó las ventajas de la tecnología.

Más tarde el tiempo demostró, que aquellas promesas no iban tan lejos. Aparecieron CD rayados, que no funcionaban, con mal sonido, etcétera. Es decir, todas las estafas que se podían hacer con un *cassette* hoy pueden hacerse con un CD. Sin embargo, los CD no bajaron de precio. Las discográficas aumentaron sus ganancias mediante el CD, o sea, gozaron de las ventajas de la tecnología.

Hoy en día, el fenómeno MP3 quizás pueda entenderse como la otra cara de la misma moneda: *quien goza las ventajas, carga con las taras*, para el caso en que los ciegos cursos causales le resulten desfavorables. La compañía discográfica acepta este principio, pero sólo referido a las ventajas.

3) *Napster y medidas autosatisfactivas: otra inaplicabilidad*. No es apropiado finalizar este trabajo sin referirnos a las medidas autosatisfactivas, un tema de enor-

[82] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-241.

[83] Palazzi, *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, *JA*, 1995-III-240.

me interés en la doctrina y jurisprudencia, debido a la situación de emergencia que atraviesa el país.

Hemos dicho en otra oportunidad que el campo de las medidas autosatisfactivas parece estar sobredimensionado en algunos casos. Allí hemos distinguido entre aplicabilidades y aplicaciones. Habíamos considerado que existe un exceso al pregonar la aplicabilidad de las medidas autosatisfactivas en el derecho penal económico (ley 25.156 de defensa de la competencia).

Si bien Peyrano[84] propone soluciones ingeniosas para casos donde se pueda sostener la aplicabilidad de una medida autosatisfactiva, consideramos que aquí estamos en una situación límite. Si un caso como "Napster" se llega a desarrollar en la Argentina, no habría casi ninguna medida autosatisfactiva que resulte aplicable. El fallo de Napster de Estados Unidos de América ha demostrado ser de cumplimiento imposible.

La solución de Napster no fue una lucha firme y sostenida "a la Ihering", sino que fue una solución "a la Orwell"[85] tal como ocurrió en la "Rebelión en la granja".

La conclusión es aquí entonces negativa: no habría medidas autosatisfactivas que puedan solucionar el fenómeno MP3. El tiempo verbal potencial da a entender, que no esperamos ni pretendemos que esta conclusión se mantenga firme por mucho tiempo.

b) Sobre el virus informático y el caso "Pinamonti"

1) *La dañosidad de los virus como criterio de demarcación*. La idea difundida entre muchos juristas de que el virus no daña la computadora sino los datos, y de que los datos son un objeto inmaterial es sólo parcialmente correcta. En verdad, hay muchos virus que atacan la información y el *software*. Pero hay una cantidad igual importante de virus, que atacan tanto a la computadora o –en términos de la decisión del caso "Piamonti"– como al soporte.

Este simple hecho a menudo no es tenido en cuenta en las argumentaciones de los juristas penales. Pero su importancia no es despreciable. Si el virus ataca a la computadora, estamos lisa y llanamente ante un delito de daño. Aquí se trata de un daño en el sentido tradicional del término. En este sentido proponemos la *dañosidad de los virus como criterio de demarcación*.

Sólo después de saber que no se trata de un virus que destruye el soporte, viene la complicada cadena argumental a favor de la penalización del delito de alteración de datos. Consideramos que en este punto posiblemente haya un defecto en la bibliografía jurídico-penal referida sobre el tema, y quizás esto no se deba a falta de conocimiento jurídico, sino a falta de conocimiento informático. La distinción entre "virus que afectan datos y programas" y "virus que afectan a la computadora" viene a ser el criterio de demarcación en esta materia.

[84] Peyrano, Jorge W. (dir.), *Medidas autosatisfactivas*, Santa Fe, Rubinzal-Culzoni, 2002.
[85] Orwell, George, *Animal farm*, versión castellana de Abraham Scheps, *Rebelión en la granja*, Bs. As., Kraft, 1955.

2) *La reforma preferible: el artículo 183 "bis" en el Código Penal*. Con respecto a la posibilidad de combatir el delito de alteración de datos, consideramos que la reforma preferible es la penalización autónoma de un tipo penal referido a la alteración de datos. Por ejemplo, la incorporación de un art. 183 *bis* en el Cód. Penal argentino.

Esto, además de ser la solución más adecuada desde el punto de vista científico y de la ley penal en el Estado de derecho, es la tendencia que hemos visto en la legislación de Alemania, Portugal, España, Chile, Italia, Estados Unidos de América, Gran Bretaña, Francia, Austria y Bolivia. En Latinoamérica, Chile y Bolivia son los países más avanzados en legislación penal sobre delitos informáticos. Le siguen Brasil y Argentina con muchos deseos y propuestas. Es de destacar, no obstante, el esfuerzo que ha comenzado a emprender el legislador argentino mediante la ley 25.326 y sus modificaciones a los delitos contra el honor y violación de secretos.