Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007

Por Pablo A. Palazzi (*)

Draft v ersión miércoles 26 de marzo de 2008.
A publicarse en la Revista de Derecho Penal y Procesal Penal, Abril-Mayo 2008, Lexis Nexis, Argentina.

(*) © 2008 Pablo Andrés Palazzi
Datos de contacto:
CABANELLAS, ETCHEBARNE, KELLY & DELL'ORO MAINI
San Martin 323, piso 17 - Buenos Aires - C1004AAG
Tel + 5411 4114-5538 - Fax + 5411 4114-5555
e-mail: p.palazzi@cekd.com – pablo@palazzi.com.ar

1. Introducción

a) Preliminar

No es la primera vez que comentamos proyectos legislativos de delitos informáticos[1]. Pero en este caso, el proyecto que analizaremos merece especial consideración pues además de ser de una excelente factura, posee el consenso en sus principales aspectos de gran parte de la industria, de especialistas, de académicos y ha recibido el respaldo de ambas cámaras del Congreso.

Por eso es prometedor que se avecine la posibilidad de que el Código Penal argentino finalmente contemple delitos relacionados con Internet y las nuevas tecnologías.

A esta altura de desarrollo de la denominada Sociedad de la Información, no sólo la mayoría de los códigos penales modernos del mundo han contemplado alguna forma de criminalidad relacionada con la informática sino que hasta existe una convención internacional sobre la materia[2] de la cual son parte mas de 40 países desarrollados, y que se encuentra en vías de ser implementada en varios de los países que la aprobaron, habiendo sido la Argentina invitada a integrarla recientemente.

Es que el delito informático ya no puede ser ignorado por el legislador: su realidad y presencia es incontrolable y los efectos devastadores que puede causar son enormes. Basta citar los millones de dólares en daños y pérdidas que ocasionan los virus informáticos, o las estafas informáticas o, para citar un fenómeno mas común, el ataque mediante denegación de servicios[3] que lleva incluso a prácticas extorsivas de ofrecimiento de servicios de seguridad a empresas en Internet. Por otra parte nuestros jueces penales que se enfrentan a estos casos se ven obligados a declarar atípicas acciones que son claramente negativas[4] y que no están contempladas en muchos casos porque el código penal fue escrito para otra época donde la información no era la materia prima del comercio y donde las actuales tecnologías de comunicación y almacenamiento y tratamiento de datos personales solo eran objeto de relatos de ciencia ficción.

b) Antecedentes

---

[1] Ver PALAZZI, Pablo, *Breve comentario a los proyectos legislativos sobre delitos informáticos*, Revista de Derecho Penal y Procesal Penal, Agosto 8/2006, pag. 1525.

[2] Convenio de Cibercriminalidad de Budapest del 23 de noviembre de 2001.

[3] Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. Chi. Legal F. 35; nota sin autor, *Love Bug, Damage Costs Rise to $ 6.7 Billion*, Computer Economics eFlash, May 9, 2000; Rob Kaiser, *Love Bug' Has Cousins; They Bite Too: Cyberattack Considered Most Disruptive Ever*, Chicago Tribune May 6, 2000, pag. 1

[4] Ver reseña de los últimos casos en PALAZZI, Pablo , *Delitos relacionados con la informática, Internet y las nuevas tecnologías*, Revista de Derecho Penal y Procesal Penal, No. 3, Noviembre de 2004, pag. 566.

En el año 2006 se desató la polémica sobre la violación de correos electrónicos de varios periodistas y jueces, a raíz de una denuncia realizada por un importante diario de la Capital. Inmediatamente se presentaron en el Congreso varios proyectos de leyes relacionados con el correo electrónico[5]. En junio del 2006 se comenzó a debatir en las comisiones de Legislación Penal, Comunicaciones y Libertad de Expresión de la Cámara baja un proyecto de modificación al Código Penal presentado por la diputada Diana Conti. La iniciativa, que igualaba la intromisión en correos electrónicos con las de misivas en papel, proponía penas de hasta diez años de prisión para la violación del correo electrónico por parte de funcionarios públicos o miembros de fuerzas de seguridad. Con el correr de los meses el Congreso cayó en la cuenta que era mejor aprovechar el interés en introducir una reforma no sólo referida al correo electrónico sino a otros delitos informáticos.

A fines del año 2006, luego de un amplio debate de sus comisiones, la cámara de diputados aprobó el proyecto de ley. El proyecto contempló los delitos informáticos mas tradicionales tales como la estafa informática, el daño informático, el acceso no autorizado a un ordenador, la falsificación de documentos digitales, y la violación de correspondencia digital, correo electrónico y cualquier otro medio de comunicación moderno así como su interrupción. También se contemplan delitos relacionados con la pedofilia y la distribución de virus informáticos.

Durante el año 2007 diversas comisiones del Senado estudiaron el proyecto de diputados. El 28 de noviembre de 2007, el Senado aprobó con reformas el proyecto de ley de delitos informáticos que había sido aprobado con media sanción el año anterior por la Cámara de Diputados.

En el Senado, las Comisiones de Justicia y Asuntos Penales y de Sistemas, Medios de Comunicación y Libertad de Expresión[6], luego de numerosas reuniones con expertos y luego de considerar otros proyectos de ley[7], emitieron un dictamen de

[5] Cfr. La nota titulada *Pretenden penar la violación de e-mails. Diputados debatirá un proyecto de ley*, diario La Nación, 4 de junio de 2006.

[6] El texto puede verse en www.senado.gov.ar buscando en "ordenes del día" la número 959/07 que contiene el dictamen de esas comisiones y los proyectos tenidos en cuenta, junto con el texto de la media sanción de la cámara de Diputados. En el recinto del Senado, el Orden del Día 959 se votó sin modificaciones, con la exposición que consta en versión taquigráfica de la Senadora Vilma Ibarra, entonces a cargo de la Comisión de Asuntos Penales del Senado.

[7] Los expedientes de proyectos legislativos que se tuvieron en cuenta en el senado fueron los siguientes: CD-109/06 - Proyecto de ley en revisión por el cual se incorporan las nuevas tecnologías como medios de comisión de distintos tipos previstos en el Código Penal; S-1751/06 - Proyecto de ley de los senadores Giustiniani e Ibarra, modificando diversos artículos del Código Penal en relación al uso privado del correo electrónico; S-1875/06 - Proyecto de ley del senador Saadi, incorporando a la legislación argentina la regulación del correo electrónico o e-mail y modificando las penas establecidas para la comisión de delitos tipificados en los artículos 153, 154, 155, 156, 157 y 157 bis del Código Penal; S-4417/06 - Proyecto de ley de la senadora Bortolozzi, estableciendo penas para los delitos electrónicos y tecnológicos; y teniendo a la vista los expedientes S-1281/06 - Proyecto de ley del senador Pichetto, modificando el art. 128 del Código Penal acerca de la protección de los niños en Internet; S-

comisiones (CD 109-06) que fue aprobado por el Senado en pleno y que se comenta seguidamente.

En líneas generales las reformas del senado al proyecto de ley originario de diputados no han hecho sino mejorarlo en su técnica legislativa y en ciertos aspectos que fueron señalados por diversos juristas y asociaciones que participaron en la discusión en las comisiones. Pero el proyecto conserva la factura inicial que le dio la Cámara de Diputados.

Se trata de una reforma al Código Penal, no de una ley de delitos informáticos. Por eso en líneas generales no se crean nuevos delitos sino que se modifican ciertos aspectos de los existentes para receptar las nuevas tecnologías.

1628/06 - Proyecto de ley del senador Jenefes y otros senadores, sobre regulación y protección jurídica del correo electrónico; S-2127/06 - Proyecto de ley de la senadora Fellner, modificando el art. 128 del Código Penal, respecto de establecer las penas por pornografía infantil; S-2218/06 - Proyecto de ley del senador Jenefes, modificando el art. 128 del Código Penal, en lo que respecta a la pornografía infantil; S-3373/06 - Proyecto de ley del senador Saadi, sustituyendo el art. 128 del Código Penal a fin de establecer las penas por el delito de pornografía infantil; S-323/07 - Proyecto de ley del senador Basualdo y otros senadores, modificando el art. 128 del Código Penal, respecto a la pornografía infantil; S-465/07 - Proyecto de ley de la senadora Escudero, reproduciendo el proyecto de ley sobre modificación del art. 128 del Código Penal fijando las penas por la difusión de la pornografía infantil (Ref.: S-1610/05); S-520/07 - Proyecto de ley del senador Jenefes, modificando el Código Penal respecto a las penas por delitos informáticos; S-809/07 - Proyecto de ley de la senadora Giusti, modificando el Código Penal, respecto a las penas por pornografía infantil; S-823/07 - Proyecto de ley de la senadora Giusti, modificando el Código Penal respecto a las penas por violación de correo electrónico; S-2021/07 - Proyecto de ley de la senadora Bortolozzi, sobre tipificación de delitos cometidos por medios electrónicos e informáticos; y S-2575/07 - Proyecto de ley de la senadora Viudes, modificando diversos aspectos del Código Penal, en relación a los delitos contra la privacidad.

2. Análisis del proyecto de reforma

2.1. Definiciones

La primera reforma propone incorporar al artículo 77 del Código Penal las siguientes definiciones:
- "El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente."

El dictamen del Senado (OD 959/2007) explica así los cambios propuestos en relación a la redacción de las definiciones: "Con respecto a la significación de conceptos se consideró de adecuada técnica legislativa unificar en una sola norma los artículos 3° y 17 del proyecto venido en revisión, y redefinir el concepto de documento, a fin de que resulte comprensivo de toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Se consideró conveniente omitir la referencia a comunicación electrónica que la sanción de Diputados traía en su artículo 3°, por considerar sobreabundante su incorporación a la parte general, por cuanto las modificaciones propuestas incluyen expresamente en los tipos penales de la parte especial del Código Penal aquella protección".

Esta reforma trae mayor coherencia al Código Penal. En efecto si bien se mantienen las definiciones existentes en la versión de Diputados se elimina la declaración del art. 3 del proyecto de la cámara baja que rezaba "*La comunicación electrónica goza de la misma protección legal que la correspondencia epistolar y de telecomunicaciones*". Esta norma resultaba sobreabundante en virtud de lo decidido en numerosos fallos[8], y del derecho vigente[9], que ya establece semejantes garantías.

[8] Ver por ejemplo: CCCFed., Sala II, 5/6/2007, Causa n° 25.062 "Ilic, Dragoslav s/ medios de prueba"; C.C.C., Sala IV, causa n° 25.065 "Redruello" del 15/11/04, y de la Sala I, causa n° 19.418 "Grimberg" del 11/2/03 y causa n° 20.009 "Yelma" del 22/4/03.
[9] Art. 18 Const. Nacional, art. 18 de la ley de telecomunicaciones y art. 5 de la ley 25.520.

2.2. El nuevo delito de ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil

Los numerosos casos de pornografía infantil que están ocurriendo, inclusive en nuestro medio local[10], así como los numerosos estudios existentes al respecto[11], demuestran que Internet se ha convertido en el medio principal para que pedófilos intercambien archivos y fotografías de menores, superando con su accionar las fronteras locales. Resulta necesario que el CP contemple esta nueva modalidad delictual, sobre todo para cumplir con los compromisos internacionales que hemos adoptado.

En nuestro país la ley 25.763 aprobó el Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño (de rango constitucional según el art. 75 inc. 22 CN). El artículo 1 de dicho Protocolo dispone que "Los Estados Parte prohibirán la venta de niños, la prostitución infantil y la *pornografía infantil*, de conformidad con lo dispuesto en el presente Protocolo". Por "pornografía infantil" se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales (art. 2 inciso "c" del referido Protocolo).

Finalmente, el art. 3 dispone que "Todo Estado Parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente: ….. ii) c) La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el artículo 2".

En lo que interesa a esta breve nota, el proyecto propone sustituir el artículo 128 del Código Penal, por el siguiente: "Artículo 128.- Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda

[10] Ver por ejemplo C. 21871 - "M., E. s/procesamiento" - CNCRIM Y CORREC DE LA CAPITAL FEDERAL - Sala I - 23/11/2004 .

[11] Fermín MORALES PRATS, Pornografía infantil e Internet: la respuesta en el código penal español, pag. 175 en Problemática jurídica en torno al fenómeno de Internet, Cuadernos de Derecho Judicial, Madrid, 2000; Luis REYNA ALFARO, Pornografía e Internet: Aspectos penales, Alfa Redi No. 50, Septiembre 2002; y David Lorenzo MORILLAS FERNÁNDEZ, Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comitivas relacionadas con Internet, Dykinson, Madrid, 2005.

representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

Esta versión del Senado es similar a la redactada inicialmente en la cámara de diputados. Pero el dictamen del Senado (OD 959/2007) propuso realizar los siguientes cambios aceptados finalmente por el pleno: "En lo que hace a los delitos contra la integridad sexual, específicamente respecto del elemento del tipo penal del artículo 128 actual, se sustituyó imágenes pornográficas por "toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales", tomando la definición del ya mencionado Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía. Hay que notar que en ninguna de las versiones finales de ambas Cámaras se incluyó la mención de actividades sexuales *simuladas*. Tal mención estaba en la versión original de la cámara de diputados[12] pero fue eliminada en un debate posterior. La idea circuló en el Senado pero por considerárselo controvertido tampoco se lo incluyó pese a que lo prevé el Protocolo Facultativo de la Convención sobre los Derechos del Niño y la Convención del Ciberdelito.

En la cámara de Diputados la reforma del art. 128 del CP había dejado de lado –por un error involuntario- la figura del que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren menores. La nueva redacción del Senado reinstala tal delito. El dictamen del Senado (OD 959/2007) explica así estos cambios: "…*se conserva en la redacción del tipo penal la conducta del que organizare espectáculos en vivo con escenas pornográficas en que participaren dichos menores, que había sido suprimida por la sanción de la Cámara de Diputados del primer párrafo del artículo 128, sustituyendo escenas pornográficas por representaciones sexuales explícitas en que participaren dichos menores*".

Finalmente, en relación al proyecto de Diputados el Senado alteró las penas que el proyecto prevé para la producción y la tenencia y se agregó un requisito mas a la

[12] Cuyo art. 128 decía "Será reprimido con prisión de uno a cuatro años el que produjere, facilitare, divulgare, financiare, ofreciere, comerciare, distribuyere o publicare por cualquier medio, toda representación de un menor de dieciocho años en actividades sexuales explícitas, reales o *simuladas*, así como toda representación de sus partes genitales con fines primordialmente sexuales".

tenencia para penalizar sólo aquella que tenga fines inequívocos de comercialización o distribución. El dictamen del Senado (OD 959/2007) explica así estos cambios "*No se consideró conveniente reprimir con la misma pena a quién distribuya representaciones de las descriptas en el párrafo anterior como a quien las tenga en su poder, ya que son ilícitos de diferente peligrosidad, y asimismo, se vigorizó la idea, en salvaguarda del principio de reserva, de requerir en forma inequívoca la finalidad por parte del autor de proceder ulteriormente a su distribución o comercialización*".

Esta nueva figura generó preocupación en las empresas que actúan como intermediarios en Internet (tales como empresas de telecomunicaciones, ISP, hosting, etc), quienes consideraron que podría llegar a imputárseles responsabilidad penal por los contenidos que transitan o se albergan (en el caso de hosting) en sus servidores, pese a que usualmente no tienen conocimiento acabado de la ilicitud del contenido en cuestión.

Entendemos que la redacción dada al tipo penal no deja lugar a dudas que estamos ante a una figura dolosa. Por ello en esos supuestos no es posible inferir que se incurra en el delito del art. 128 CP. Para ello nos basamos en lo siguiente: (i) no existe conocimiento efectivo de los contenidos y de su ilicitud; (ii) en la mayoría de los casos no podría existir tal conocimiento por la inviolabilidad de las comunicaciones; (iii) sumado a la inexistencia de un deber de vigilancia o supervisión de contenidos[13]. En todo el derecho comparado se considera a ésta como una figura dolosa, como lo han resuelto expresamente tribunales españoles[14].

Asimismo por ser una figura de tenencia o posesión, se ha planteado en doctrina y jurisprudencia el problema de los usuarios que poseen en sus discos una imagen sin conocimiento de dicha posesión. Aquí nuevamente la falta de dolo hace que no exista delito. Tal supuesto se daría en el caso de un usuario que "baja" directamente de Internet (o a través de una red *peer to peer*) un archivo zipeado sin conocer su contenido en el entendimiento que es una película o archivo musical según el título del archivo, pero que luego resulta que contiene imágenes prohibidas por el art. 128 CP. EN este caso entendemos que tampoco habría presencia de la finalidad de distribuir o comercializar que exige el segundo párrafo del art. 128 CP.

También podría darse el supuesto de un usuario adulto que solamente visualiza esas imágenes online (acción que el art 128 CP no prohíbe) sin grabarlas, pero que por la configuración técnica del ordenador quedan grabadas en la memoria *cache* del

[13] Para un desarrollo de este deber en el ámbito penal ver Manuel GOMEZ TOMILLO, *Responsabilidad penal y civil por delitos cometidos a través de internet. Especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces*, Thomson-Aranzadi, segunda edición, pag. 123.
[14] Ver por ejemplo sentencia del Tribunal Supremo español 1553/2000 de 10 de octubre (RJ 2000/9151).

navegador sin su consentimiento. En estos supuestos, y dado el contexto del caso, la jurisprudencia norteamericana sostuvo en el caso "US v. Stulock"[15] que no se daban los elementos del tipo penal de tenencia de imágenes de pornografía infantil. A similares conclusiones llegó la doctrina[16].

2.3. Violación de Secretos y de la Privacidad

a) Nuevo epígrafe para el Código Penal: el derecho a la privacidad

La reforma del Senado conservó la propuesta de la Cámara de Diputados de ampliar el epígrafe del capítulo III, del título V, de la parte especial del Código Penal, incluyendo a la "privacidad" como bien jurídico protegido. Explica el dictamen del Senado que "*sobre todo a tenor de lo prescripto por el inciso 3 del artículo 157 ("3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales"), ya que la norma se entiende más como afectación a la intimidad que al bien jurídico secreto*". El art. 153 bis propuesto también refuerza la protección de este bien jurídico en ambientes digitales.

La modificación no podía ser mas acertada. El bien jurídico penalmente protegido es el determinado previamente como tal por una comunidad ubicada en el tiempo y en el espacio, que, por decirlo de alguna manera, elige qué entidad merece ser considerada como bien por satisfacer sus necesidades individuales y sociales[17]. Pues bien, no cabe duda que las nuevas tecnologías han aumentado los riesgos y peligros para el derecho a la privacidad. Hoy en día existen cientos de bases de datos con nuestros datos personales; nuestros rastros e imágenes digitales quedan en numerosos lugares en la web, en videocámaras de ingreso a edificios, en estadios y edificios públicos, en tarjetas de ingreso a oficinas, en correos electrónicos y comunicaciones por chat, en búsquedas en Internet, mensajes de texto telefónicos (SMS) y mensajería instantánea. La gente y la sociedad son concientes de todo ello. Se han aprobado marcos legales para ponerle límite al uso que se haga de estos datos tales como el habeas data en la reforma constitucional del año 1994 o la ley de protección de datos personales, pero constantemente nos encontramos con nuevos casos de robo de identidad, sustracción de información personal o venta masiva de bases de datos personales. Ante todo este panorama, el derecho penal debe acompañar estos

[15] 308 F.3d 922, 924 (8th Cir. 2002). La corte de apelaciones dijo "one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically saved in the browser's cache, without having purposely saved or downloaded the image".
[16] Matthew James Zappen, *How Well Do You Know Your Computer? The Level of Scienter in 18 U.S.C. 1462,* 66 Alb. L. Rev. 1161, 1165-76 (2003); Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227 (2004).
[17] GOSCILO, Antonieta, *Los bienes jurídicos penalmente protegidos*, en Lecciones y Ensayos, Segunda Epoca, 1, Temas de Derecho Penal II, Diciembre 1981, pag. 25.

cambios con nuevas normas que se adecuen a la realidad tecnológica actual pero también con nuevos bienes jurídicos que conceptualicen esas necesidades.

b) Violación de correspondencia digital

El proyecto sustituye el artículo 153 del Código Penal, por el siguiente: "Artículo 153.- Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una *comunicación electrónica*, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una *comunicación electrónica*, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una *comunicación electrónica* que no le esté dirigida".

Se agrega asimismo un párrafo que dispone "En la misma pena incurrirá el que *indebidamente* interceptare o captare *comunicaciones electrónicas o telecomunicaciones* provenientes de cualquier sistema de carácter privado o de acceso restringido".

Tal como actualmente reza el actual artículo 153 se prevé que "La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica" (se reemplaza culpable por autor y se agrega la mención de "comunicación electrónica").

Se agrega además que "Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.". La razón de este párrafo final se explica por el origen que tuvo el proyecto, destinado a evitar la interceptación y acceso no autorizado a correos electrónicos de jueces y periodistas según se difundió ampliamente por la prensa a mediados del año 2006.

Salvo por lo dispuesto en este último párrafo, el proyecto que comentamos no innova creando nuevos tipos penales, sino que a los existentes les agrega el término "comunicación electrónica" para actualizarlos

La reforma resuelve el problema de la atipicidad de la violación de correspondencia electrónica. Algunos tribunales habían considerado atípicas las acciones realizadas sobre correos electrónicos[18]. Y si bien en el caso "Lanata" se concluyó que el correo electrónico podía ser equiparado a la correspondencia tradicional en los términos de

[18] Ver por ejemplo el fallo correccional dictado por la Juez Dra. Ana Diaz Cano respecto al apoderamiento de un correo electrónico de una cuenta de hotmail. Disponible online en http://www.habeasdata.org/node/249

los arts. 153 y 155 CP[19], la lectura del fallo dejaba un sabor de interpretación analógica de la ley penal. Una cosa es sostener que la garantía constitucional de la correspondencia se aplica al correo electrónico a los fines de aplicarle todas las garantías constitucionales que resguardan a un medio de comunicación personal y otra cosa distinta es considerar que es delito "abrir" un correo electrónico sin permiso. Por eso toda la doctrina planteó la necesidad de una reforma legislativa[20].

La redacción final dada al tipo penal del art. 153 CP es cuidadosa. En efecto, la palabra "indebidamente" aparece repetida cuatro veces en el texto, algo un tanto sobreabundante a primera vista (en el texto vigente del art. 153 aparece sólo dos veces). Nos parece acertada su inclusión pues si bien a primera vista puede considerarse innecesaria, coincidimos con la doctrina que al comentar el tipo original señaló "en este caso, como en otros, la expresión (indebida) tiene el sentido de fundar el delito sobre una firme y delineada figura objetiva y subjetiva de licitud que excluye toda posibilidad de imputar el delito en forma culposa"[21]. Es decir, esta figura sigue siendo un delito doloso.

Con esta aclaración quedan salvadas las objeciones de ciertos medios empresarios que abrigaban el temor que esta figura penal fuera aplicada a acciones de un proveedor de acceso a Internet o de servicios de mail tales como desviar un correo electrónico porque contiene un virus o porque un algoritmo o filtro lo clasifica como spam. No es la finalidad de la nueva figura prevista en el art. 153 del CP el penalizar tales situaciones. Pero además nunca podría llegarse a tal resultado interpretativo por la carencia de dolo en tal accionar. Asimismo cabe resaltar que el término "indebido" es también sinónimo de realizado sin derecho[22]. En tal sentido, un ISP o proveedor de servicio de correo, está en su derecho, según sus términos y condiciones de uso, de desviar o etiquetar correspondencia no solicitada (spam) que es ilegal en Argentina[23], o de suprimir aquella que constituya una amenaza para su seguridad o la de sus usuarios si contiene virus o algún programa potencialmente dañino.

---

[19] JA 1999-III-237; ED 182-478.

[20] RIQUERT, *Protección Penal de la intimidad en el espacio virtual*, pag. 105; D´ALESIO, Andrés José (Director) y DIVITO, Mauro (Coordinador), Código Penal comentado y anotado, parte especial, pag. 361; sin embargo ver Gustavo ROMANO DUFFAU, *Protección penal del contenido del email*, en Cuadernos de Propiedad intelectual, tomo I, 2004, pag. 307, sosteniendo que bajo el texto actual podía incluirse el correo electrónico.

[21] SOLER, Sebastián, *Derecho Penal Argentino*, tomo 4, pag. 121, TEA, 1992.

[22] D´ALESIO, Andrés Jose (Director) y DIVITO, Mauro (Coordinador), Codigo Penal comentado y anotado, parte especial, pag. 359.

[23] Ver art. 27 ley 25.326 y caso de spam "Tanus v. Cosa" publicada en los siguientes medios: La Ley 2006-C-281; Jurisprudencia Argentina, semanario del 7 de junio de 2006; MicroJuris, documento MJJ7137, comentado por Flavio FARINELLA, titulado *Algunas notas sobre el spamming* (documento MJD2896); El Dial, del 27 de abril de 2006 y El Dial, 30 de mayo de 2006, y en Revista jurídica Zeus, Abril 2006, con nota de Jorge PRIVIDERA, Spam, cobertura legal en la Ley de Protección de Datos Personales.

Ello se ve corroborado por el dictamen del Senado (OD 959/2007) que fundamenta así estas conclusiones: "Con respecto al actual artículo 153 del Código Penal, última parte del primer párrafo *(… suprimiere o desviare de su destino una correspondencia que no le esté dirigida*) es razonable la propuesta de la Cámara de origen de incorporar no sólo la comunicación electrónica sino también la expresión "indebidamente" en el tipo, para que no le queden dudas al intérprete respecto a requerir la finalidad dolosa del autor del delito, y evitar cualquier hermenéutica tendiente a considerar comprendidos en el tipo a quienes en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección para evitar lo que se conoce como spam, o la recepción de correos no deseados por sus clientes". La voluntad del legislador es clara en cuanto excluir de las conductas típicas a estos supuestos: no incurre en delito quien desvía un mail porque es un correo electrónico no solicitado o porque contiene un virus.

c) Acceso ilegítimo a un sistema informático

La reforma incorpora como art. 153 bis del Código Penal, el siguiente: "Artículo 153 bis. Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

En otra ocasión analizamos la importancia de esta figura[24], y señalamos además la falta de adecuación típica en nuestro sistema legal conforme lo acreditaron numerosos fallos[25]. Cabe señalar que son numerosas las jurisdicciones que penalizan el acceso ilegítimo a sistemas informáticos pues estos suelen ser la antesala para la comisión de otros delitos como la estafa, el daño, la sustracción de datos personales, de claves o de secretos comerciales. En esa inteligencia, el legislador estableció que solo resultará de aplicación esta figura "*si no resultare un delito más severamente penado*".

El texto legal hace referencia a "sistema o dato informático de acceso restringido" puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet público (como son la gran mayoría).

[24] Ver El acceso ilegítimo a sistemas informáticos: la urgente necesidad de actualizar el código penal, JA 1999-III-321.
[25] Ver el fallo publicado en JA 1999-III-321 y el caso del acceso ilegítimo a la página web de la Corte Suprema de Justicia de la Nación, comentado por RIQUERT, Delitos Informáticos, en la obra Derecho Penal de los Negocios, Astrea, (Daniel Carrera y Humberto Vazquez, directores) pag. 303.

Esta disposición causó inicialmente alarma en más de un programador que consideró que la norma en cuestión podría aplicarse al *ethical hacking* o al testeo que expertos de seguridad realizan de las falencias de redes informáticas mediante software herramientas de software dedicadas a tal fin (acceder sin permiso, pescar claves, puertos abiertos en una red u ordenador, etc.). Esto último puede tener lugar en el caso de investigación académica, casera y empresaria sobre virus informáticos, empresas de seguridad que testean sistemas de bloqueo, *firewalls*, y un largo etcétera de usos lícitos que pueden tener estas tecnologías de "hacking ético". En la práctica, si ocurre con consentimiento del dueño o titular de la red que está siendo testeada, existe una autorización legal por parte de la "víctima", con lo cual no se da el elemento del tipo que requiere que el acceso ocurra "sin la debida autorización o excediendo la que posea". Esta autorización puede tomar cualquier forma, pero generalmente se verá reflejada en un contrato de servicios de seguridad informática.

Cabe aclarar también que esta figura no está destinada a prohibir la ingeniería inversa (o ingeniería reversa). El objetivo de la ingeniería inversa es obtener información técnica a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado. Los productos más comunes que son sometidos a la ingeniería inversa son los programas de computadoras y los componentes electrónicos[26]. Por ejemplo un usuario legítimo puede abrir un programa informático con el fin de corregirle un error o permitir que corra en otro sistema operativo, o abrir un contenido (ej. un DVD) para poder leerlo en otra plataforma si está encriptado originariamente, o en la consola de la competencia, o "abrir" un teléfono celular para poder hacerlo funcionar en otro proveedor distinto o abrir una rutina de filtrado de contenidos en Internet para averiguar que sitios filtra y "si filtra de más o de menos" sitios inocentes. El listado de acciones es interminable.

Como es dable observar, todas de esas situaciones están relacionadas con la protección de la propiedad intelectual (tales como el derecho de autor o patentes, que este proyecto no tratan), mientras que el bien jurídico protegido por la figura que estudiamos (art. 153 bis del CP) es la privacidad. Por ende, partiendo del objeto de la protección penal, está claro que cualquier intento de utilizar esta figura para frenar un acto de ingeniería inversa no debería tener recepción judicial. De hecho la ley de patentes contiene excepciones para experimentación antes del vencimiento de la misma.

[26] http://es.wikipedia.org/wiki/Ingenier%C3%ADa_inversa

Finalmente lo relativo a las medidas de protección tecnológica, que limitan en cierto modo la ingeniería inversa, fue introducido en el Tratado de Derecho de Autor de la OMPI del año 1996, que nuestro país aprobó oportunamente, pero que todavía no reglamentó ni en el ámbito civil ni en el ámbito penal. En Estados Unidos en cambio fueron legisladas en la ley conocida como *Digital Millennium Copyright Act* (DMCA) y cuya aplicación en algunos casos puntuales fue muy controvertida[27]. Ahora bien, la Corte Suprema fue muy clara en el caso "Autodesk" (CSJN, sentencia del 32/12/98) en cuanto a que un tratado internacional no alcanza para crear un delito (en el caso se trataba de la reproducción de programas de ordenador sin autorización de su autor) y que para que haya delito se requiere una ley del Congreso. Al no haber ley del Congreso que en forma específica sancione penalmente la ingeniería inversa (lo cual podría considerarse una pésima decisión de política legislativa), mal podría aplicarse el tipo penal del art. 153 bis del CP a estos casos.

d) Publicación abusiva de correspondencia

Se actualiza el art. 155 siguiendo la misma técnica del art. 153 reformado (agregado del término *comunicación electrónica*). La nueva redacción del artículo 155 del Código Penal reprime con multa al "que hallándose en posesión de una correspondencia, *una comunicación electrónica*, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere *publicar* indebidamente, si el hecho causare o pudiere causar perjuicios a terceros".

Así como es grave violar la privacidad de una correspondencia mediante su acceso o interceptación, también lo es el publicar el contenido de una carta o correo electrónico que se supone debe quedar en la esfera íntima y no ser divulgada. Es por ello que también el proyecto actualiza esta norma permitiendo que se sancione a quien *indebidamente* publique tanto una correspondencia tradicional como la digital. Cabe preguntarse si seguirá vigente aquello que la doctrina señalaba respecto a que, en esta figura, el concepto de publicar una cosa es ponerla al alcance de un número indeterminado de personas, pero la comunicación privada y personal, aunque sea a un cierto numero de personas no es suficiente[28].

Se agrega la disposición que no se encuentra en el actual art. 155 del CP y que reza: "Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público". La norma, reproduciendo claramente la idea subyacente en el art. 111 inc. 1 del CP para las calumnias, busca eximir de responsabilidad penal a quien revela una correspondencia cuyo contenido es de claro

[27] Ver un claro resumen en Electronic Frontier Foundation, *Las Consecuencias No Deseadas: Cinco Años Bajo la Digital Millennium Copyright Act*, Revista Chilena de Derecho Informático. N°4, Mayo de 2004 pp 17-35 disponible en http://www.derechoinformatico.uchile.cl

[28] SOLER, ob citada, tomo IV, pag. 133.

interés público. La disposición en cuestión es razonable e incluso resulta entendible en el contexto en que se sancionó esta norma. Recordamos que los medios de prensa estuvieron detrás de la sanción inicial de esta norma, a raíz de las violaciones de correo electrónico ocurridas en el año 2006 a varios periodistas.

e) Revelación de secretos

En consonancia con las reformas de los arts. 153 y 155 se sustituye el artículo 157 del Código Penal, por el siguiente texto: "Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos *o datos, que por ley deben ser secretos*." Se agrega el término datos para actualizar esta figura y proteger penalmente los daos que están en poder de la administración pública y que por ser secretos no deben ser revelados a terceros.

f) Unificación de los tipos penales de los arts. 117 bis y 157 bis del CP: acceso a un banco de datos, revelación de información y alteración de datos

El proyecto de reforma modifica el artículo 157 bis del Código Penal, por el siguiente:
"Artículo 157 Bis.- Será reprimido con la pena de prisión de un mes a dos años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."

El Senado consideró de adecuada técnica legislativa unificar los artículos 9 y 10 del proyecto de Diputados (que establecían los delitos de insertar datos falsos y revelar información de un banco de datos respectivamente) en una sola norma, ya que ambos refieren a modificaciones del artículo 157 bis Código Penal.

Al unificar las normas del art. 117 bis y del art. 157 bis CP en una sola además se propone derogar el art. 117 bis pues existía coincidencia que en ciertos casos no protegía el honor pese a su ubicación. El dictamen de la cámara alta explica así esta unificación: "A tenor de la incorporación en el artículo 157 bis de la conducta

consistente en insertar o hacer insertar datos en un archivo de datos personales, y teniendo en cuenta la similar regulación del artículo 117 bis, inciso 1°, en Título Delitos contra el Honor (Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales) se consideró acertado modificar la ubicación metodológica dentro del Código Penal, ya que en una ulterior revisión del tema se llegó a la conclusión que la norma se encuentra mal ubicada dentro de los delitos contra el honor". Para llegar a esta conclusión el dictamen del Senado cita un reciente fallo donde se sostuvo: "*Pareciera que la conducta reprochada podría encontrarse alcanzada por las previsiones legales del artículo 117 bis. Sin embargo, si bien este artículo en su inciso 1° reprime con pena de prisión de un mes a dos años al que "...insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.", no puede soslayarse su ubicación sistemática dentro del Código Penal, por lo que si tenemos en cuenta el bien jurídico protegido por el título la nueva figura parece limitarse sólo a la inserción de datos falsos que disminuyan el honor. Por tal motivo, la única interpretación adecuada del citado artículo, es la de considerar que contempla las acciones que desacreditan o deshonran, pese a que ello no surge del texto de la ley*"[29]. Adhiriendo a este razonamiento, y para no incurrir en redundancias penales, ya que la amplitud del nuevo tipo penal proyectado abarca la tipicidad de la conducta expresada por el inciso 1° del artículo 117 bis del Código Penal, el dictamen del Senado explica que se consideró pertinente su derogación.

Hay que resaltar que estos tipos penales introducidos por la ley 25.326 de protección de datos no fueron muy eficaces y están sujetos a controversias de diversa clase. Sin entrar en profundidad a todas las cuestiones, señalamos que nunca se aclaró si eran delitos de acción pública o de acción privada. Se entiende que los delitos de violación de secretos son acciones privadas (art. 73 CP), salvo los casos de los arts. 154 y 157, excepciones que obedecen a que el Estado tiene interés en que siempre se persiga a los sujetos que tienen responsabilidades asignadas y el 157 bis quedará dentro de este supuesto, ya que "si el legislador hubiera querido incluirlo dentro de las excepciones así lo habría previsto expresamente en la ley 25.326"[30]. En igual sentido se planteó el dilema con el art. 117 bis CP, que no se encuentra enumerado dentro de los delitos de acción privada (el art. 73 CP hace referencia solo a calumnia e injuria). La jurisprudencia ateniéndose al texto del Código consideró que no eran acciones privadas[31]. Sin embargo cierta doctrina entiende que la interpretación

[29] CCC Fed. Sala I 17.4.2007 "MARTINEZ RODRIGUEZ, Hugo R. y otros".
[30] D´ALESIO, Andrés Jose (Director) y DIVITO, Mauro (Coordinador), Codigo Penal comentado y anotado, parte general, pag. 735.
[31] CNCrim y Correc, Sala V, 12/11/2002, revocando la decisión de un juzgado correccional que consideró al art. 117 bis CP como de acción privada (ver Jdo. Correc. N.11, causa 6151 "Citibank NA s/art. 117 bis Cód Penal").

sistemática de las normas llevaría a concluir que las conductas descriptas por el art. 117 bis CP son perseguibles solamente mediante la acción privada[32].

g) Captación ilegal de datos, imágenes y sonidos

La norma contenida en el artículo 6° del proyecto aprobado por la Cámara de Diputados establecía en forma muy amplia un delito que consistía en la obtención o captación de la imagen, sonidos o datos de una persona en forma ilegal y su posterior difusión. El Senado prefirió no incluir este delito en el proyecto.

El dictamen del Senado (OD 959/2007) explica así esta eliminación: "La norma contenida en el artículo 6° del proyecto aprobado por la Cámara de origen fue cuestionada, porque se infiere de la misma la punición de las *cámaras ocultas*, lo que se consideró merecedor de otro debate en cuanto no se encuentra directamente vinculado a la materia de esta iniciativa: incorporar las nueva tecnologías al Código Penal. Asimismo, el texto de este artículo mereció observaciones respecto de la introducción del verbo típico "obtuviere" por cuanto ello implicaría extender la punición a límites exagerados, ya que en tanto no sea difundido, revelado o cedido el dato o hecho captado, la lesión al bien jurídico protegido es prácticamente insignificante".

El proyecto en su versión de Diputados podría haber impactado en los medios de investigación periodísticos, sobre todo en el periodismo investigativo y en el uso de cámaras ocultas para detener y dar a conocer casos de corrupción. Asimismo habría creado controversias con las actuales medidas de video-vigilancia existentes en el sector público y privado. También podría haber sido usado en casos de agencias de investigación y detectives privados para poner coto a invasiones a la privacidad, aunque a veces estas investigaciones pueden ser legítimas si se realizan dentro del marco legal. Hay que reconocer que la propuesta de diputados era muy amplia y si bien estamos a favor de proteger penalmente la vida privada de las personas de la forma mas amplia posible, hay otros valores como la libertad de expresión, de prensa y de informar que no deben imponerle limites irrazonables.

En el derecho comparado las cámaras ocultas han sido controvertidas, habiéndose admitidos en algunas decisiones judiciales su uso por parte de la prensa[33] y considerado ilícitas en otras[34], sobre todo porque en muchas situaciones significan

[32] D´ALESIO, Andrés Jose (Director) y DIVITO, Mauro (Coordinador), Código Penal comentado y anotado, parte especial, pag. 153.
[33] Ver el caso estadounidense "J.H. Desnick v. ABC, Inc.", 44 F.3d 1345 (7th Cir. 1995). El fallo considera que la cadena de televisión ABC no invadió la privacidad cuando usó cámaras ocultas para filmar a un odontólogo que realizaba prácticas inecesarias y engañaba a sus pacientes sometiéndolos a operaciones y tratamientos falsos.
[34] En el caso "Food Lion v. Capital Cities/ABC, Inc.", 194 F.3d 505 (4th Cir. 1999) un jurado otorgó la suma de 5,5 millones de dólares en daños punitivos pero el tribunal de apelaciones luego lo redujo a sólo 350,000 dólares

una avance no consentido sobre la propiedad o la privacidad de terceros[35]. Pero esto no significa que la solución sea penalizar su uso.

2.4. Estafa informática

El proyecto propone como nuevo inciso 16 del artículo 173 del Código Penal, el siguiente: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.". Se sigue así la línea doctrinaria que propone incorporar estas situaciones patrimoniales abusivas como estafa dado el dilema que existía en relación las interpretaciones judiciales[36].

Así lo fundamenta el Senado al expresar en su dictamen conjunto de comisiones: "…con relación al "fraude informático" existió coincidencia en cuanto a la conveniencia de incorporarlo dentro del capítulo sobre las defraudaciones, y despejar definitivamente las dudas suscitadas en los tribunales sobre en qué tipos de delitos contra la propiedad debe subsumirse la conducta".

Pero a diferencia de la redacción de Diputados, el Senado clarifica tanto los medios como el *iter criminis*. Se explica así la propuesta de cambio "Se conservó la redacción de la sanción de Diputados con dos supresiones: "actuado sin autorización del legítimo usuario", porque se entendió que agrega un elemento al tipo que resulta confuso e innecesario, ya que la autorización no podría excluir la ilicitud de la conducta de defraudar; y "luego de su procesamiento", porque no se encontró el justificativo de fijar el momento técnico de una etapa de la transmisión de datos. Por ello en el … presente dictamen no se discriminan esos momentos, dando al juzgador precisión normativa y evitando elementos típicos que lo pudieran hacer incurrir en confusión".

2.5. Daño informático

El art. 10 del proyecto incorpora como segundo párrafo del artículo 183 CP, el siguiente: "*En la misma pena incurrirá el que alterare, destruyere o inutilizare*

---

por el suo de cámaras ocultas para armar un programa de televisión en el cual se denunciaban supuestas prácticas insalubres en supermercados que luego no resultaron ser tales.

[35] Gyong Ho Kim, *Extreme Departure Test as a New Rule for Balancing Surreptitious and Intrusive Newsgathering Practices with Competing Interests: The Use of Hidden Cameras vs. the Right to Be Let Alone*, UCLA Entertainment Law Review, Vol. 10, pag. 213 (2003).

[36] Ver estos casos en D´ALESIO, Andrés José (Director) y DIVITO, Mauro (Coordinador), Código Penal comentado y anotado, parte especial, pags. 458/459; y de nuestra autoría: ¿Hurto simple o estafa por medio de computadoras?, LL 1994-B-441 y en "Derecho de la Alta Tecnología" (DAT) N° 51-18 (año 1992); Apoderamiento de dinero de un cajero automático", ED, 171-571; y Algunas modalidades delictivas relacionadas con el uso de ordenadores y cajeros automáticos", en Derecho de la Alta Tecnología No. 109, Año X, septiembre de 1997.

datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Con esta norma de proyecto se soluciona el problema que se había generado en la jurisprudencia que consistía en considerar atípica la destrucción de datos o programas de ordenador[37] o incluso la difusión de virus informáticos en redes de computadores[38]. La modificación del Senado mantiene la misma pena que para el daño común[39].

Los verbos típicos son "alterare, destruyere o inutilizare". Si bien difiere del "daño común" pues se agrega el término "alterare", entendemos que no hay mucha diferencia con los conceptos previstos en el tipo penal original. Alterar sería modificar un archivo de datos o programa sin destruirlo completamente.

En el contexto informático, destruir o inutilizar quiere decir borrar definitivamente sin posibilidad de recuperación. La respuesta a si esto ocurre o no en un caso concreto dependerá del sistema informático y operativo utilizado. En la mayoría de los sistemas operativos la acción de borrar no implica que el hecho se produzca indefectiblemente, pues los archivos borrados se almacenan en una carpeta conocida como basurero o *trash can*. Generalmente para poder concluir la acción de borrado de datos el usuario debe reconfirmar el borrado para eliminar los documentos e incluso en estos casos es posible recuperarlos en algunas situaciones. Por ende la consideración de la destrucción debe ser analizada caso por caso. Existen otras formas de borrado mediante virus informáticos, o programas dañinos que pueden "saltearse" estas seguridades impuestas por los sistemas operativos. También cabría la posibilidad de destruir el hardware (generalmente de menor valor) con la finalidad de destruir los datos o software (de mayor valor).

El hecho que exista un sistema de *back up*, como sucede en la mayoría de las empresas en modo alguno altera el delito de daño pues la restauración requiere un esfuerzo que ya implica reparar el daño causado.

---

[37] Ver reseña de casos en nuestro trabajo *Virus Informático y Delito de daño*, Revista de Derecho Penal y Procesal Penal, Abril 4/2006, pag. 674 y en especial el caso "Pinamonti" con nuestro comentario *La destrucción de programas de computación y el delito de daño (La necesidad de una reforma legislativa y su propuesta)*, en JA, 1995-III-236.

[38] Ver nuestra nota Virus Informáticos y responsabilidad Penal, LL 1992-E-1122.

[39] En los Fundamentos para el dictamen del CD-109/06 se explica que "Se coincidió en incorporar el "daño informático" al Código Penal, pero con la pena prevista en la figura básica del delito de daño, ya que ni el medio técnico utilizado para dañar ni el objeto sobre el que recae, pueden ser considerados por si solos un elemento agravante. Salvo, claro está, que se trate de un daño contra un determinado bien que merezca especial protección, circunstancia que ameritaría introducirlo en las previsiones del artículo 184 Código Penal con una pena agravada".

El delito puede recaer sobre "datos, documentos, programas o sistemas informáticos". Esta es la principal modificación que requería nuestro código penal. La ausencia de tales objetos en la descripción del art. 183 CP llevó en numerosos casos a concluir que su destrucción resultaba atípica.

Además del daño informático tradicional se agrega una nueva modalidad de daño. Se penaliza a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Se entiende que estos programas, como por ejemplo un *virus maker* o herramientas específicas de destrucción de datos, son potencialmente dañosas. Por ende quien de alguna manera pone en el comercio un programa de tales características, con conocimiento del daño a producir, ayuda de alguna manera a cometer el delito de daño a quien usará la herramienta.

El proyecto, sin embargo, no prohíbe la existencia de estos programas, sino que penaliza a quien los venda, los distribuya o los haga circular o introduzca concretamente en un sistema informático. La redacción da a entender que sería un delito de peligro abstracto, y por ende no requerirá un daño concreto. Entendemos sin embargo que como se sigue exigiendo la presencia de dolo, y en especial del dolo específico de dañar[40] (no basta incluso una voluntad genérica: debe tratarse de una intención clara y manifiesta). No quedan aprehendidas por esta figura las conductas donde no hay dolo de dañar.

En cuanto a la posibilidad de incriminar a quienes producen una herramienta que puede eventualmente usarse para crear daños informáticos, el tema se platea con las llamadas tecnologías de doble uso, de las cuales vemos miles de ejemplos en la vida cotidiana: la fotocopiadora, la video casetera, un equipo "doblecasetera", un ipod, un disco rídigo, una grabadora de dvd, el software *peer to peer*, y un largo etcétera de software y hardware que permite copiar obras intelectuales, reproducirlas, difundirlas. Tanto doctrina como jurisprudencia[41] coinciden ampliamente en que estas tecnologías no son ilegales ni susceptibles de ser prohibidas si tienen usos sustancialmente legítimos o no infractores, aunque de paso también tengan usos no legítimos[42]. La solución legal mas razonable en estos casos es permitir la existencia

[40] La jurisprudencia mayoritariamente ha requerido un dolo especifico en el delito de daño. Ver ROMERO VILLANUEVA, Horacio, Código Penal de la Nación anotado, pag. 823, Lexis Nexis, 2006, segunda edición ampliada y actualizada.

[41] Así lo decidió la Corte Suprema de Estados Unidos en el caso "Sony" (464 U.S. 417; 104 S. Ct. 774; 78 L. Ed. 2d 574; 1984 U.S. LEXIS 19; 52 U.S.L.W. 4090; 220 U.S.P.Q. (BNA) 665; 224 U.S.P.Q. (BNA) 736).

[42] En el caso Sony citado en nota anterior la Corte Suprema de Estados Unidos concluyó: "The sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes, or, indeed, is merely capable of substantial noninfringing uses".

de estas herramientas y solamente sancionar su uso en un caso concreto cuando este uso sea ilícito pero permitiendo que coexistan los usos legítimos. Por ende si el programa destinado a causar daños encuentra un uso legítimo, tal uso no será ilegal, en cambio si no es posible encontrarle usos legítimos o que no produzcan daño, no se ve porque no debería prohibirse su distribución.

También esta figura tan amplia de daño informático plantea otros problemas para la protección de la propiedad intelectual cuando se utilizan programas anticopia que dañan, degradan o limitan el funcionamiento del sistema informático. Veamos.

Si un programador inserta un virus en un programa a fin que, en caso de copia, el mismo se active y destruya la información existente en el ordenador es posible considerar la situación como un daño informático además de un abuso de derecho (art. 1071 Código Civil). Si bien el titular de la obra de software está en su derecho de proteger sus intereses como autor o dueño (arts. 1 y 5 ley 11723), dicha facultad no debe extenderse más allá de lo que razonablemente expliciten las leyes, o el contrato que lo relacione con el usuario. Así, cabe plantearse la situación de que el sistema de seguridad anti-copia –conocidos generalmente como dispositivos de "*self-help*"- sólo se limite a borrar o detener el programa no original (la copia ilícita) dejando intactos los datos del usuario. En tal situación el productor de software no está -a nuestro entender- infringiendo norma de derecho penal alguna para el caso que haya previsto esta facultad en el contrato de licencia, y no haya transferencia de propiedad del software ni de las copias. Si bien en otra ocasión sostuvimos que la vía correcta en ese caso sería demandar judicialmente el secuestro y destrucción de la copia ilegítima, luego de revocar la licencia[43], un nuevo examen de la cuestión nos convence de que no resulta necesario recurrir a acción judicial alguno si esto está previsto en el programa adecuadamente.

No creo que este tipo penal pueda aplicarse a los recursos informáticos que inhabilitan o degradan el sistema operativo en caso de copia ilegal de un sistema operativo o programa de ordenador limitando su propia funcionalidad.

Ello es así porque la finalidad de este delito es penalizar al que daña con la intención de alterar datos o sistemas informáticos, por lo que requiere un dolo específico de dañar que no es compatible con la situación comentada, que constituye una legítima defensa de la propiedad intelectual[44]. Aunque claramente en estos casos se suele hablar de legítima defensa de la propiedad (art. 34 inc. 3 CP), entendemos que ni

[43] PALAZZI, Virus informático y delito de daño, Publicado en Rev. Derecho Penal y Procesal Penal , Abril 2006 no. 4, pags. 674

[44] Permitida hasta cierto punto y en lo que a medidas de protección tecnológicas se refiere por el tratado de Derecho de Autor de la OMPI, suscripto por Argentina.

siquiera ello sería aplicable por no haber delito si no se daña información, software o hardware de terceros y por ende no es necesario recurrir a una causal de excepción[45].

La mejor guía para arribar a esta conclusión es interpretar el bien jurídico protegido del delito de daño que es la propiedad. Sabemos que no hay delito si no está afectado el bien jurídico protegido. En estos casos el software pertenece al titular de los derechos de autor que dispone la protección tecnológica determinada (por ej. inhabilitar funciones, ubicar carteles recomendando comprar el original, o hacer mas "lento" o degradar el sistema operativo). Por ende, la propiedad del dueño del ordenador no está afectada ni destruida. No existe el daño sobre bienes propios (el art. 183 CP dice "total o parcialmente ajeno").

Finalmente, la supuesta víctima no podría alegar que su máquina se encuentra disminuida en su funcionalidad cuando la causa de ello es su propio accionar ilegal que consiste en copiar y usar una obra intelectual -programa de ordenador- sin la autorización de su titular[46], lo que genera la falta de funcionamiento pleno del sistema.

Los fabricantes de software suelen recurrir a estos dispositivos de protección como una medida antipiratería. Obviamente, estas medidas disgustan mucho a los usuarios[47], y hasta hacen incómodo el uso de sistemas informáticos pero son perfectamente legales en la medida en que no se afecte materialmente el hardware o se destruyan datos, programas o contenidos ajenos.

El proyecto de reforma agrega como agravante al Art. 184 CP el siguiente: "Artículo 184.- La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes: … 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."

2.6. Daño a las comunicaciones

[45] Aunque siempre son buenas las analogias con otras situaciones, nos parece dificil encontrar alguna en tal sentido. Pero imagine el lector un auto o una casa que como protección cuando detercan que alguien está adentro en forma no autorizada se bloquean e impiden la salida de quien ingresó furvicamente. ¿Podría ser ello considerado privación ilegal de la libertad?

[46] Lo que de paso constituye otro delito penal: art. 72 de la ley 11.723.

[47] Ver la nota *Microsoft retira un polémico recurso antipiratería*, en Clarin, 4/12/2007. La nota explicaba que la herramienta, al detectar una copia ilegal del Windows Vista, inhabilitaba el sistema operativo. Ahora, ante las quejas de los usuarios, quienes utilicen programación ilegal sólo recibirán advertencias constantes y sugerencias para acceder a la original, pero no perderán funcionalidades, disponible en http://www.clarin.com/diario/2007/12/04/um/m-01556748.htm

Hemos dado este título a la nueva figura propuesta en el Art. 197 CP porque consideramos que al incluir cualquier clase de comunicación (y no sólo las antiguas telegráficas y telefónicos) la figura no sólo ampara lo público sino cualquier clase de comunicación incluyendo las privadas como el correo electrónico, la voz a través de IP, o los mensajes de chat o de texto a través de celulares (SMS).

Esta reforma es importante porque el tipo anterior, como había dicho la doctrina, estaba teñido de la idea de lo público, ya que lo que se protege es la seguridad pública y en esa situación era muy difícil pensar en tipicidad cuando se trataba de redes de uso particular o privado como por ejemplo intercomunicación telefónica en un establecimiento rural[48]. Lo que quiso el legislador es ampliar el tipo penal a esos nuevos medios de comunicación con independencia de su naturaleza pública o privada.

El proyecto propone entonces que el nuevo Art. 197 quede redactado así "Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida."

Se trata de una figura dolosa, sobre todo en lo relativo al verbo resistir. No cabe entonces incluir dentro de este tipo de delitos a supuestos de caída de redes o sistemas de comunicaciones por diversos problemas técnicos, ajenos a la intención del operario técnico. Sí en cambio quedarán incluidos los ataques por denegación de servicios

4. Conclusiones

Esta reforma probablemente requerirá en el futuro de nuevos debates y actualizaciones, pero es muy importante que haya tenido lugar debido a que el Código Penal por su antigüedad no contemplaba ninguna de estos delitos informáticos clásicos.

Uno de los puntos que quedó en claro en este debate es que el sector empresario relacionado con las nuevas tecnologías tiene una gran resistencia a la regulación legal de cualquier clase, incluso de una regulación destinada a amparar su infraestructura informática como lo hace este proyecto. Esto plantea la necesidad de estudiar normas de resguardo sobre la inmunidad o exclusión de responsabilidad de ciertos sectores como los intermediarios de Internet o aquellos relacionados con la informática.

***

[48] CREUS, Derecho penal, pag. 51; D´ALESIO, Andrés José (Director) y DIVITO, Mauro (Coordinador), Codigo Penal comentado y anotado, parte especial, pag. 631.