MINISTERIO PÚBLICO DE LA DEFENSA
Secretaría General de Capacitación y Jurisprudencia

CONSULTA DESTACADA

JURISPRUDENCIA

Agosto de 2016

Delitos informáticos

ÍNDICE

i. Camara Federal de Apelaciones de San Martin. Sala I. "Inc. de apelación del procesamiento de Baroni". Causa Nº 327/13. Reg. Nº 9504. 7/6/2013.

Defraudación por medios informáticos. Tipicidad. Perjuicio patrimonial.

j. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VI. "taringa.net y otros". Expte. 41181.6. 29/4/2011.

Ley de propiedad intelectual. Internet. Auto de procesamiento.

k. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VI. "G. R. y otro". Causa Nº 39.779. 3/8/2010.

Defraudación por medios informáticos. Phishing. Tipicidad..

l. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala I. "N, C". Expte. 38137.1. 5/5/2010.

Daño. Auto de procesamiento. Reforma legal. Principio de legalidad. Cracking.

m. Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal. Sala I. "Campero, FJ". Falta número de causa. 17/12/2008.

Ley de marcas y patentes. Dominio de Internet. Tipicidad. Sobreseimiento.

n. Juzgado en lo Correccional Nº1 de Bahía Blanca. "Faraoni, JM". Causa Nº 1060/15. 1/6/2015.

Grooming. Tipicidad.

o. Tribunal Oral en lo Criminal de Necochea. "Fragosa, LN". Expte. T.C. Nº 4924-0244. 5/6/2013.

Grooming. Tipicidad.

a. Cámara Federal de Casación Penal. Sala III. "Oliva, A". Reg. Nº 1366/15. Causa Nº 43.128/2012. 20/8/2015.

Retención indebida. Tipicidad. Software. Interpretación de la ley. Sobreseimiento.

- Hechos

El juzgado de instrucción había sobreseído a una persona por el delito de retención indebida. La decisión fue, a su vez, confirmada por la Cámara de Apelaciones. Contra esa resolución, la querella interpuso recurso de casación. Se discutía, esencialmente, los términos en los que un programa informático podía ser considerado "cosa mueble" de conformidad con lo establecido en el artículo 173, inciso 2º del Código Penal.

- Decisión y fundamentos

La Sala III de la Cámara Federal de Casación rechazó el recurso y confirmó el sobreseimiento.

"[L]a doctrina y la jurisprudencia unánimemente han exigido, como elementos típicos [del art. 173 inc. 2º]: una omisión dolosa ('*negarse a restituir o no restituir*'), un plazo para cumplir con dicha obligación ('*a su debido tiempo*'); y que el accionar del autor provoque un perjuicio patrimonial para el dador u otra persona (resultado que, en definitiva, se requiere para toda defraudación).

[…]

[N]o se advierte la verificación de aquellos presupuestos objetivos que reclama la infracción normativa contemplada por el art. 173, inc. 2 del C.P., ya que el reclamo de este caso no está constituido por una cosa mueble, sino por un programa informático que nunca fue recibido por el nombrado con cargo de oportuna devolución, ya que resultaba un programa creado por él mismo, es decir, de su exclusiva propiedad intelectual (Ley 11.723), extremo reconocido inclusive por el propio denunciante.

[E]l conflicto traído a inspección sólo se resume en una controversia respecto de la titularidad de aquellos desarrollos que el encausado hubiere producido en el uso del software de su propiedad intelectual 'Luxevent', sin poder identificar cual sería la cosa mueble, 'causa fuente de obligaciones' que Agustín Oliva debía restituir" (voto del juez Borinsky al que adhirieron los jueces Catucci y Riggi).

b. Cámara Federal de Casación Penal. Sala III. "Castelo, PA". Causa Nº 51772/2011. 16/6/2015.

Defraudación por medios informáticos. Tipicidad. Prueba. Prueba- apreciación.

- Hechos

El Tribunal Oral condenó a una persona a una pena de prisión por defraudación mediante técnicas de manipulación informática. La maniobra había consistido en ingresar a una cuenta de homebanking ajena, transferir dinero a la cuenta de un tercero para retirarlo con posterioridad. Contra esa decisión, la defensa interpuso recurso de casación. Entre otras cuestiones, se impugnó la autoría y la capacidad del condenado de realizar la maniobra defraudatoria.

- Decisión y fundamentos

La Sala III de la Cámara Federal de Casación rechazó el recurso.

"Con relación a la autoría [del condenado] en el hecho investigado, [se] destacó que la circunstancia de que la transferencia sobre la cuenta de [CMB] del Banco Francés se haya dispuesto de un IP situado en Guadalajara, México, no es óbice para endilgarle la maniobra defraudatoria denunciada.

En dicho sentido, destacaron que 'de acuerdo a la nueva tecnología de que dispone cualquier persona con conocimientos de informática puede operar un 'IP' situado en otro país desde la República Argentina, tal como se explica, incluso, mediante tutoriales en internet […] que brindan instrucciones no sólo para navegar con un IP de otro país sino también para hacerlo en forma anónima, esto es, sin poder ser identificado'.

[L]os magistrados de la instancia anterior refirieron que del informe de la firma 'Google Inc.' surge que la cuenta de correo de [PAC] se hallaba vinculada a 'direcciones de IP extrañas a la jurisdicción Argentina'.

[L]a incapacidad técnica alegada por la defensa de [PAC] para realizar la manipulación informática que se le atribuyó, no se corresponde con las tareas que desempeñaba en 'Global Logic' (que lo muestran conocedor de lo que 'hay detrás de una página de internet') y su carácter de estudiante universitario de ingeniería en sistemas de la UBA.

La conclusión alcanzada por el tribunal de juicio en torno al punto también encuentra apoyo en los dichos de [DOA], quien señaló que en la firma 'Global Logic' poseían

herramientas y software adecuado para trabajar con páginas web que requerían de usuarios y contraseñas" (voto de la jueza Catucci, al que adhirieron los jueces Riggi y Gemignani).

c. Cámara de Apelaciones en lo Criminal y Correccional Federal. Sala I. "NN". Causa Nº CFP 4669/2015. 7/9/2016.

Violación de secretos. Daño informático.

- Hechos

Se le atribuía a una persona haber accedido ilegalmente a la cuenta de Youtube de un partido político, modificar la contraseña y subir vídeos difamatorios. El juzgado de instrucción declaró extinguida la acción penal por desistimiento de la parte querellante. Contra esa decisión, la querellante interpuso recurso de apelación.

- Decisión y fundamentos

La Cámara Federal, pese a que no formaba parte de los motivos de agravio, resolvió que los hechos encuadraban en el delito de daño informático y revocó la resolución.

"[E]l primer tramo de la conducta, el ingreso no autorizado al sistema, corresponde al tipo penal por el cual se interpuso la querella –art. 153 bis–, mientras que las conductas desarrolladas con posterioridad resultarían, en principio, compatibles con el comportamiento tipificado en el segundo párrafo del artículo 183 del Código Penal.

Al respecto, entiendo que corresponde descartar el delito regulado en el artículo 153 *bis* del C.P., pues 'se trata de una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización' […].

En este orden de ideas, es dable mencionar que 'acceder por cualquier medio a un sistema o dato informático de ingreso restringido conforme el art. 153 bis del CP', suele ser la antesala para la comisión de otros delitos de estafa, daño, la sustracción de datos personales, de claves o de secretos comerciales.

[E]l legislador estableció que sólo resultará de aplicación esta figura 'si no resultare un delito más severamente penado'. Si están presentes alguno de los delitos mencionados, éstos desplazan a la figura de acceso ilegítimo de un sistema o dato informático' […]. Así, 'cuando el fin buscado es destruir o cambiar el contenido de la información', se está ante la presencia de otro tipo penal…" (voto del juez Freiler, al que adhirió el juez Farah).

d. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala IV. "Jiménez, DM.". Causa Nº 76339/14. 15/5/2015.

Violación de secretos. Desestimación por inexistencia de delito. Hacking. Tipicidad.

- Hechos

El gerente de recursos humanos de una compañía fue denunciado por enviar –desde su correo electrónico laboral– información confidencial de su empleadora. La fiscalía y la querella intentaron imputarle el delito de acceso ilegítimo a un sistema informático. El juzgado de instrucción desestimó la denuncia por inexistencia de delito. Contra esta decisión, ambos acusadores interpusieron recursos de apelación.

- Decisión y fundamentos

La Sala IV de la Cámara Nacional de Apelaciones confirmó la desestimación de la denuncia.

"Acerca del tipo penal de acceso ilegítimo a un sistema informático incorporado por la Ley 26.388, comúnmente denominado hacking, la conducta típica se basa en el acercamiento por parte del sujeto activo, llamado usualmente hacker, a información contenida en un dispositivo automatizado para cuyo acceso se requiere un permiso especial […].

Los presupuestos del caso traído a estudio exhiben que no nos encontramos frente a esa figura, pues a partir del rol que cumplía el causante en la compañía al tiempo en que se habría producido el acceso a la información […], se deriva sin hesitación que se encontraba autorizado a acceder a los datos relacionados con los haberes percibidos por los empleados. Ergo, el objeto sobre el que recae la acción atribuida a J. no se adecua a las previsiones del artículo 153 bis del Código Penal, en tanto esa información no poseía carácter restringido para el querellado.

Tampoco se adecua el hecho al tipo del hurto simple, del artículo 162 del referido ordenamiento, caracterizado por la acción de apoderarse de un bien total o parcialmente ajeno.

Partiendo de la teoría de la *ablatio*, en punto a la interpretación del verbo que distingue a esta calificación legal, se ha dicho que el hurto radica en el desplazamiento del sujeto

que puede realizar actos de disposición, hurtar sería entonces usurpar el poder sobre la cosa […].

[L]os archivos en cuestión no fueron 'desplazados', ya que no solo nunca salieron de la esfera de custodia del sujeto pasivo, sino que 'S. A. I. S. A.' tampoco perdió poder […] de disposición sobre esa información, que permaneció almacenada en los dispositivos de la compañía. Su supuesto envío por parte de J. a una casilla de correo electrónico de uso personal no importa entonces la acción de apoderarse que distingue al tipo de hurto" (voto de los jueces González Palazzo y González).

e. Cámara Federal de Apelaciones de Córdoba. Sala A. "Avila, AA y otro". Expte. Nº FCB32020028/2012. 3/7/2014.

Violación de correspondencia. Tipicidad. Sobreseimiento.

- Hechos

El juzgado federal de primera instancia había sobreseído a dos personas con funciones en la División Análisis – Investigación en las Comunicaciones de la Policía de la provincia de Córdoba por el delito de falsificación de documento público. Se les atribuía, en este punto, haber participado en la confección de oficios judiciales irregulares a fin de obtener información de ciertos números telefónicos. Contra aquella decisión, el fiscal interpuso recurso de apelación. Allí, alegó que la conducta de los imputados podía constituir violación de correspondencia.

- Decisión y fundamentos

La Cámara Federal confirmó el sobreseimiento.

"[L]a conducta endilgada a los imputados […] no encuadra en las acciones típicas descriptas por el artículo 153, en ninguna de sus variantes. Específicamente en lo que nos convoca, el segundo párrafo del art. 153 del C.P. comprende dos conductas penalmente típicas, a saber, la interceptación de comunicaciones electrónicas o telecomunicaciones y su captación.

[De la consulta del] significado de [las] acciones [enumeradas en el art. 153 CP] en el Diccionario de la Real Academia Española surge por un lado que la tercera acepción del verbo **interceptar** implica '*Interrumpir, obstruir una vía de comunicación*" y que la tercera acepción del verbo **captar** significa '*Recibir, recoger sonidos, imágenes, ondas, emisiones radiodifundidas*'.

[S]e advierte que la [metodología utilizada por los imputados] no implica ni la interceptación ni la captación de comunicaciones telefónicas, en tanto no interrumpieron ni obstruyeron vías de comunicación ni tampoco receptaron las ondas emitidas por ellas, sino que su accionar se habría limitado a solicitar a distintas compañías información relacionada a ciertos números telefónicos. Tal como lo indicaron las defensas técnicas […], no hubo intervenciones telefónicas propiamente dichas, sino que sólo se habría intentado recabar datos sobre ciertas líneas telefónicas, tales como la titularidad, teléfonos de referencia y contactos, pero sin haberse

adentrado en el contenido propio de las llamadas entabladas entre tales líneas y otras" (voto del juez Vélez Funes, al que adhirieron los jueces Muscará y Rueda).

NOTA: Los jueces Muscará y Rueda, además, sostuvieron que "…conforme surge del artículo 73 del Código Penal, el delito de violación de secretos (a excepción de los tipos penales previstos por los art. 154 y 157 del C.P.) es un delito de acción privada, es decir que la acción respecto de éste no puede iniciarse de oficio, sino que requiere inexorablemente el impulso del agraviado o de su representante legal. […] En el caso bajo estudio, las partes, incluido el señor Fiscal General ante la Cámara, han reconocido y hecho expreso que los titulares de las líneas telefónicas son desconocidos a la fecha, es decir que los supuestos damnificados con la obtención de los distintos datos permanecerían en el anonimato y por lo tanto nadie habría tenido la posibilidad de promover la acción privada".

f. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VII. "Blanco, R". Causa Nº 70199/13. 6/5/2014.

Violación de secretos. Delito de acción privada. Querella.

- Hechos

El juzgado de primera instancia determinó que la querella presentada en el proceso era inadmisible por no cumlir con la exigencia de "formulación de imputación penal" (art. 418 CPPN) y que el delito previsto en el art. 153 *bis* del CP era de acción privada. La decisión fue impugnada por la pretensa querellante que alegó que el art. 73 CP –que regula las acciones privadas– alude a la violación de secretos y no al delito contemplado en el art. 153 *bis* CP.

- Decisión y fundamentos

La Sala VII de la Cámara Nacional de Apelaciones confirmó la decisión de primera instancia.

"[L]a acción que nace del delito previsto en el artículo 153 *bis* citado ciertamente es de acción privada (artículo 73, inciso 2°, del ordenamiento sustantivo).

Debe recordarse en tal sentido que aun con motivo de la reforma operada por la ley 26.388, el legislador mantuvo la exclusión de los arts. 154 y 157 del Código Penal en la enumeración del mencionado art. 73, inciso 2º, de modo que al no quedar incluida en la excepción, la figura del art. 153 *bis* ha quedado abarcada en aquellas cuya acción es privada.

La falta de inclusión del novel tipo penal –acceso ilegítimo a un sistema o dato informático–, entonces, en las excepciones de los arts. 154 y 157, parece pauta más segura que aquella que se vincula con el título del capítulo, máxime frente a la aproximación del tipo en estudio, en algunas características, con una de las figuras del art. 153 –violación de correspondencia electrónica–, cuyo ejercicio de la acción también es privado.

[De acuerdo al debate parlamentario,] las modificaciones propuestas 'están vinculadas con temas que la norma penal ya tiene contenidos en su seno. En ese sentido, hablaremos no ya de violación de secretos, sino de violación de secretos y privacidad. Debemos dejar en claro que el bien jurídico a proteger es el de la privacidad,

equiparando en algún sentido la comunicación electrónica con la correspondencia epistolar'.

[E]n el debate de las nuevas disposiciones –que incluyó la discusión del art. 153 ter, finalmente no sancionado– se sostuvo que 'el artículo 73 del Código Penal establece en su inciso 2° que la violación del secreto es una acción privada, salvo en el caso de los artículos 154 y 157. O sea que esto no se estaría modificando porque estamos incorporando distintos incisos al artículo madre, que es el de violación de secretos'"(voto de los jueces Cicciario y Divito).

g. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala V. "P., L. y otros". Causa Nº 13630/2012. 28/10/2013.

Ley de propiedad intelectual.
Internet. Sobreseimiento. Riesgo permitido.

▪ Hechos

Un grupo de personas administradoras del sitio Youtube.com habían sido denunciadas por delitos derivados de la ley de propiedad intelectual. Se les atribuía haber permitido que se reprodujeran obras cinematográficas en el sitio *web* sin el consentimiento de los titulares de ese derecho. El juzgado de instrucción sobreseyó a todos los denunciados. Contra esta decisión, la querella interpuso recurso de apelación.

▪ Decisión y fundamentos

La Sala V de la Cámara de Apelaciones confirmó el sobreseimiento.

"[Según] surge de las constancias documentadas [...] y de los términos de la declaración de M. A. J., de la División Delitos Tecnológicos de la Policía Federal, www.youtube.com es una página de reproducción de los archivos en formato de video que son subidos a esa plataforma por usuarios registrados, desde la cual, quienes no lo son pueden verlos gratuitamente y sin cumplir ningún requisito. Según explicó, para incorporar un archivo de esas características al sitio se requiere estar registrado como usuario; agregó que, de hecho, al ejecutar la acción la plataforma asigna a esa persona –que puede estar en cualquier parte del mundo– una identificación única, que sirve para encontrar el video en cuestión (enlace). Es decir, que se trata, en principio, de una plataforma sin contenidos, en la que básicamente es el usuario quien lo provee [...].

La característica esencial es que los contenidos que se suben a YouTube no son conocidos anticipadamente por los que administran el sitio y, de hecho, en la mayoría de los casos provienen de filmaciones de particulares, ediciones privadas, o de medios periodísticos, o de la decisión positiva de difusión gratuita por parte de quienes tienen derechos reconocidos sobre una obra, etc.

En ese contexto, [...] no tiene cabida la pretensión de la querella de considerar *ex ante* a los explotadores del sitio como garantes de los contenidos de esa página y/o partícipes necesarios de las acciones delictivas o ilegales que se puedan realizar a través de la incorporación de los videos que se suban. La eventual acción dolosa o negligente de estos usuarios (por ejemplo, en casos de difusión de pornografía infantil,

defraudaciones, acoso, difamación, etc.) no puede regresar convirtiendo en delictivo el tramo común objeto del contrato –la puesta a disposición de la plataforma y el uso que realiza el que se registra– porque la prestación del servicio consiste en facilitar una herramienta cuyo uso ilegal no puede, como se dice, alcanzar al que la facilita.

El sitio web cuya responsabilidad la querella pretende criminalizar, que reproduce videos on line, esto es, presta un servicio de intermediación para subir contenidos y su característica esencial para socializar información cultural a nivel mundial le otorgan una condición destacada. Esto pone en evidencia que, si bien nos encontramos frente a una actividad riesgosa, por los beneficios mencionados precedentemente en la difusión y promoción de contenidos culturales, es aceptada como un riesgo permitido […].

En consecuencia, los efectos que pueda tener la utilización ilegal o ilícita del sitio sólo podrán generar alguna responsabilidad posterior, una vez que los titulares del sitio tengan conocimiento de ello. [S]i bien no tiene la obligación de controlar la ilegalidad de los contenidos, salvo supuestos expresamente establecidos por políticas de la empresa o por acuerdos que haya suscripto, deben colaborar con posterioridad con los titulares de los derechos para que, identificada la infracción, se proceda a retirarlos del sitio. La responsabilidad del sitio recién se hará presente, ex post, cuando el que invoca el carácter de titular de un derecho lo puso efectivamente en conocimiento, individualizando en concreto los contenidos que pueden lesionar o restringir sus derechos […].

Si la cuestión [fuera] polémica en sede civil, resulta claro que la responsabilidad objetiva por el peligro de la cosa, que podría, eventualmente, acarrear responsabilidades civiles conforme al art. 1113 del Código Civil, no puede ser importada al derecho penal" (voto del juez Bruzzone, al que adhirieron los jueces López González y Argerich).

h. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala V. "Pemow, M y otros". Causa Nº 36742/2011. 24/10/2013.

Defraudación por medios informáticos. Phishing. Autoría mediata. Sobreseimiento

▪ Hechos

La firma Banelco había denunciado a un grupo personas por el delito de "phishing". A tres de ellas se les atribuía haber modificado las claves de *homebanking* de las víctimas para luego transferir dinero a cuentas de terceros. Para ello, pudo identificarse que las operaciones registraban sus direcciones de IP como el lugar desde el que se había efectuado la conexión a Internet para realizar la maniobra. En sus descargos, los tres negaron los hechos. Coincidentemente, el perito de la División de Delitos Tecnológicos de la PFA explicó que este tipo de maniobras son realizadas por expertos en informática, que se encuentran en distintas ubicaciones geográficas y utilizan habitualmente direcciones de IP ajenas a través de virus o troyanos sin permiso ni conocimiento de sus titulares con el fin de que no se descubra el verdadero origen de la operación. A otro grupo de personas se les atribuía la percepción de ese capital en sus cuentas personales y su posterior giro al exterior por servicio postal. En su indagatoria, indicaron que habían sido contactados por correo electrónico o personalmente a fin de trabajar como agentes de transferencia. La labor consistía en recibir dinero de distintas fuentes (donaciones y pagos) y girarlo a España. A su vez, manifestaron que habían sufrido sustracciones de dinero de sus propias cuentas bancarias.

El juzgado de instrucción sobreseyó a todos los imputados. Contra esta decisión, la fiscalía y la querella interpusieron recursos de apelación.

▪ Decisión y fundamentos

La Sala V de la Cámara de Apelaciones confirmó el sobreseimiento.

"[N]os encontra[mos] frente a un claro caso de lo que en materia informática se conoce como phishing, técnica utilizada por distintas agencias criminales multinacionales para la obtención ilícita de datos sensibles –en el caso cuentas bancarias de terceros– que, manipulados en forma remota, permiten el acceso a sistemas informáticos ajenos en los que los autores logran operar libremente y en beneficio propio, y en evidente perjuicio a sus verdaderos titulares.

[Respecto del segundo grupo de personas, se deduce que] todos han sido víctimas de una misma maniobra delictiva en la cual actuaron -engañados- como meros

instrumentos que obraron sin dolo de los verdaderos autores del ilícito que, de ser detectados, serán considerados autores mediatos. Al respecto, ha explicado la doctrina que 'el rasgo fundamental de la autoría mediata reside en que el autor no realiza personalmente la acción ejecutiva, sino mediante otro (instrumento); y lo que caracteriza el dominio del hecho es la subordinación de la voluntad del instrumento a la del autor mediato', que en este caso en particular se verifica a través de la relación laboral simulada.

En este mismo contexto, 'la primera hipótesis de la autoría mediata se da en el caso del que utiliza, como medio para alcanzar el fin propuesto, a otro cuya acción –por el contrario- no se dirige al mismo fin del autor mediato sino a uno distinto cualquiera. El dolo del instrumento faltará siempre que éste obre con error o ignorancia sobre las circunstancias del tipo'.

[E]l idéntico modus operandi detectado en cada una de las maniobras nos lleva a concluir que se trató de una estafa masiva en la que los 'agentes de transferencia de dinero', figura bajo la cual se simuló la contratación de estas personas, fueron inducidos a error mediante un engaño para lograr el apoderamiento patrimonial indebido, en perjuicio de los titulares de las cuentas bancarias afectadas.

[E]l modus operandi desplegado por los verdaderos autores -que aún se desconocen- se repite de igual forma en todos los casos: obtención de datos de cuentas bancarias mediante la inserción de virus informáticos, contratación simulada de agentes de transferencia de dinero, giro de dinero a Barcelona, España, a nombre de terceros y a través de empresas de correo postal privadas como 'Western Union'.

[Respecto de ellos, se puede] concluir que obraron de buena fe y sin conciencia de ilicitud, máxime si se tiene en cuenta también que otros tantos se comunicaron directamente con sus bancos y autorizaron el regreso de esos fondos depositados en sus cuentas a sus verdaderos titulares.

[De este modo, no] se ha podido acreditar el elemento subjetivo del tipo penal en juego" (voto de los jueces López González, Argerich y Bruzzone).

i. Camara Federal de Apelaciones de San Martin. Sala I. "Inc. de apelación del procesamiento de Baroni". Causa Nº 10.540. Reg. Nº 9504. 7/6/2013.

Defraudación por medios informáticos. Tipicidad. Perjuicio patrimonial.

▪ Hechos

El juzgado de instrucción había procesado a una persona por el delito de defraudación por medios informáticos. Las maniobras fraudulentas consistieron en el envío de varios correos electrónicos desde la casilla de la víctima, originados en IPs pertenecientes al imputado y a su mujer, que tuvieron como consecuencia la transferencia de dominios de Internet al imputado. Contra esta decisión, la defensa interpuso recurso de casación. Entre otras cuestiones, discutió la existencia de perjuicio económico como requisito necesario para configuración de la estafa.

▪ Decisión y fundamentos

La Cámara Federal de San Martín confirmó el procesamiento.

"La figura penal en trato, al igual que en todas las formas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona. En el caso, la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso […].

[En el caso,] a través de una manipulación informática -acceso por cualquier medio y sin la debida autorización a una cuenta de correo electrónico del querellante- se provocó la transferencia de un activo con contenido apreciable económicamente (dominios de Internet) en perjuicio del patrimonio de [la víctima] y en beneficio del imputado. Esta maniobra fue la que habría permitido que el organismo administrador de los nombres de dominio bajo el código país haya dado comienzo al proceso electrónico de transferencia. Aclarando que cualquier medida posterior a ese pedido que se hubiese llevado a cabo no habría impedido el traspaso de los dominios […].

Con relación a la falta de acreditación del perjuicio económico, este tendrá lugar cuando el sujeto pasivo se vea privado de un elemento integrante de su patrimonio por

obra de la acción delictiva, cuya disminución resulta evaluable económicamente, lo que se verificaría en el expediente" (voto de los jueces Fernández, Fossati y Soto).

j. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VI. "Taringa.net y otros". Expte. 41181.6. 29/4/2011.

Ley de propiedad intelectual.
Internet. Auto de procesamiento.

- Hechos

El juzgado de instrucción había procesado a dos personas por poseer una firma que prestaba el servicio de *hosting* para un portal de internet que ofrecía a usuarios anónimos la posibilidad de compartir y descargar gratuitamente distintas obras sin el consentimiento de sus autores. Contra esta decisión, la defensa interpuso recurso de apelación.

- Decisión y fundamentos

La Sala VI de la Cámara de Apelaciones confirmó el procesamiento.

"La reproducción ha sido definida como el modo de llevar a cabo la multiplicación material en cualquier forma o por cualquier medio de objetos corporales idénticos o similares […].

Los imputados a través de su sitio permitían que se publiciten obras que finalmente eran reproducidas sin consentimiento de sus titulares […]. Si bien ello ocurría a través de la remisión a otro espacio de Internet, lo cierto es que justamente tal posibilidad la brindaba su servicio.

[…]

Adviértase que si bien los autores del hecho finalmente serían aquellos que subieron la obra al *website* y los que 'la bajan', lo cierto es que el encuentro de ambos obedece a la utilización de la página Taringa, siendo sus responsables al menos partícipes necesarios de la maniobra y además claros conocedores de su ilicitud, por lo que el convenio que exhiben para pretender exonerarse de responsabilidad no podrá ser tenido en cuenta" (voto de los jueces Lucini y Filozof).

k. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala VI. "G. R. y otro". Causa Nº 39.779. 3/8/2010.

Defraudación por medios informáticos.
Phishing. Tipicidad.

- Hechos

El juzgado de instrucción había procesado a dos personas por estafa informática. Se les imputaba haber sustraído dinero de la cuenta bancaria de la víctima a través de un *software* con el que la engañaron para que informara el número de su cuenta y sus claves de transferencia. La defensa interpuso recurso de apelación.

- Decisión y fundamentos

La Sala VI de la Cámara de Apelaciones confirmó el procesamiento.

"[L]a circunstancia que el dinero de R. haya ingresado en la cuenta de G. al día siguiente de la obtención de los datos, mediante la manipulación informática (página paralela) denunciada […] es suficiente como para agravar [su] situación procesal […].

Que no se hayan verificado, en el caso, todos los pasos del procedimiento del 'Phishing' como alega especialmente la asistencia técnica de G. o que no se haya determinado de qué computadora se realizó las transferencias, no altera de momento los graves indicios cargosos.

Sólo resta consignar la dinámica informática –público y notorio– y que G. como lo certifica la copia del diploma aportado es perito mercantil con orientación en computación…" (voto de los jueces Lucini y Filozof).

I. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala I. "N, C". Expte. 38137.1. 5/5/2010.

Daño. Auto de procesamiento. Reforma legal. Principio de legalidad. Cracking.

▪ Hechos

El juzgado de instrucción había procesado a una persona por haber eliminado archivos del sistema informático de una empresa. En el recurso de apelación, la defensa argumentó que la conducta era atípica pues, a la fecha de comisión del hecho, no se encontraba vigente el art. 183 *bis*, que introdujo el daño informático como delito.

▪ Decisión y fundamentos

La Sala I de la Cámara Nacional de Apelaciones confirmó el procesamiento.

"[E]n cuanto a la alegada Tipicidad, si bien es cierto que este hecho habría sido cometido con anterioridad a la sanción de la ley 26.388 (4/6/08, B.O. 25/6/08) que introdujo el delito de daño informático –art. 183, segundo párrafo, CP–, lo que impide su encuadre legal en dicho tipo por el principio *nulla poena sine lege*, consideramos que encuadra en el delito de daño, previsto en el primer párrafo de la citada norma.

[M]ás allá de la reforma, nos enrolamos en el sector de la doctrina y jurisprudencia que consideraba que un hecho como el denunciado ya encontraba adecuación en el tipo previsto por el art. 183, primera parte CP pues, además de lo oportunamente resuelto [...], cabe señalar lo expuesto por Rodrigo F. Caro (El archivo almacenado en soporte informático como objeto del delito de daño', LA LEY, 2004-A, 1436) en cuanto a que la información se almacena en el soporte a través de un campo magnético. De este modo, luego de ferromagnéticas que lo componen están esparcidas al azar. Para organizarlas se utilizan pulsos eléctricos a través de una bobina enrollada alrededor de un núcleo de hierro; dicho conjunto forma la cabeza de lectura/escritura, ubicada a escasa distancia de la superficie del disco. Así el campo magnético inducido por la bobina sobre el núcleo pasa a la superficie y magnetiza las partículas, forzándolas a alinear sus polos positivos con negativos. De esta manera, la cabeza crea una banda magnética sobre el disco, y, próxima a ésta, una segunda; juntas, representan un bit. Si ambas bandas se alinean en la misma dirección, representa un cero; caso contrario, un uno. Este proceso de constitución lógica del disco, como vemos, se encarga de agrupar el conjunto de bits en estructuras de datos que tengan significado dentro del maremagnum de efectos magnéticos que existen en el interior del disco. De todo esto tenemos que los cabezales

escriben los datos al alinear partículas magnéticas sobre las superficies del soporte. A su vez, los cabezales leen datos al detectar las polaridades de las partículas que de tal modo se han alineado. Así los datos se almacenan mediante pequeños cambios en la imanación, en uno y otro sentido y según el enseña que los datos se almacenan de manera organizada en unidades de asignación denominadas clusters, la cual sólo podrá ser ocupada por un archivo -nunca dos diferentes-.

La información de este modo almacenada en la computadora ocupa un espacio: existe, no de una manera perceptible por el ojo humano sino a través de la tecnología, en el caso, representada por cabezales de lectura/escritura y confirmando su presencia física, también es transportable electrónicamente.

Sin duda es una obra humana que se puede detectar, aprehender, destruir o eliminar. Solo que, puntualmente este modo de existir, es una determinada conformación magnética. Entonces, es aceptable pensar que al destruir o inutilizar -a través de un virus- o al hacer desaparecer –mediante el borrado– un archivo de computadora –como campo magnético conformado tecnológicamente– se estaría dañando una cosa en el sentido del tipo previsto en el art. 183 del Cód. Penal, en tanto es objeto del delito un elemento detectable materialmente.

Finaliza indicando que su propuesta es perfectamente aplicable a la comisión del delito a través de Internet, modalidad conocida como sabotaje informático –cracking– constitutiva de una conducta dirigida a menoscabar la integridad y disponibilidad de la información desde una computadora que accede a través de una conexión remota; tal como sucedió en el caso a estudio.

A mayor abundamiento, Pablo A. Palazzi en su artículo ya citado comenta, entre otros, el precedente ‘Marchione’ de la Sala IV de la Cámara Nacional de Casación Penal (rta: 18/3/05) y que un sistema operativo se compone del hardware y del software o programa de ordenador. Este último es el componente lógico o ‘intangible’ del sistema informático, y que el procedimiento del imputado consistió en alterar ese conjunto de instrucciones logrando que el hardware ejecutase órdenes que se tradujeron en acciones nocivas, no aprobadas por sus legítimos usuarios, siendo el ejemplo más claro el borrado de archivos de datos insertos en el disco rígido.

Así, entendiendo ambos como una unidad compleja tangible-lógica, la afectación de uno implica al del otro, por lo que concluye que éste sí reúne los requisitos de cosa en el sentido del art. 2311, CC, ya que está compuesto -además de una parte intangible- de una parte claramente material, soporte físico” (voto de los jueces Bruzzone y Rimondi).

m. Cámara de Apelaciones en lo Criminal y Correccional Federal. Sala I. "Campero, FJ". Causa Nº 43.163. 17/12/2008.

Ley de marcas y patentes. Dominio de Internet. Tipicidad. Sobreseimiento.

▪ Hechos

Dos personas habían sido denunciadas por el delito de estafa. Se les atribuía haberse registrado en el Network Internet Center de Argentina bajo un dominio de Internet cuya marca (Technicals) era propiedad del denunciante. La jueza de instrucción sobreseyó a ambos imputados por considerar que no utilizaron el dominio ni obtuvieron beneficios del registro. Contra esta decisión, el denunciante constituído en querellante, interpuso recurso de apelación.

▪ Decisión y fundamentos

La Sala I de la Cámara Federal de Apelaciones confirmó el sobreseimiento.

"[C]abe señalar que no obran en la causa informes registrales del Instituto Nacional de Propiedad Industrial sobre 'Technicals', tampoco surge de la denuncia la existencia de ese nombre como marca. En este sentido, la tutela penal de los derechos protegidos por la ley 22.362 necesariamente requiere la previa y efectiva inscripción, motivo por el cual, la acreditación del registro correspondiente resulta insoslayable para la persecución penal. Al respecto, el tribunal ha dicho que 'la sola registración de un dominio realizada ante 'Network Information Center Argentina' (N.I.C. Argentina) para que se incorpore una página web a la red internet no lesiona ningún bien jurídico protegido penalmente por las leyes 22.362 y 11.723. No es posible en el ámbito penal equiparar un dominio a una marca' (c. 37.327 'Albertochi, Darío s/procesamiento', rta. 6/12/05, reg. 1417).

Sentado ello, corresponde analizar si la conducta enrostrada a los imputados podría encuadrar en una figura penal distinta a la regulada en la ley 22.362.

[…]

[A]ún en la hipótesis de que [el hecho] perturbara el derecho del querellante respecto del uso del dominio adquirido, no surge de autos que pueda ser considerado siquiera como actos preparatorios de una infracción penal.

En tal inteligencia, entendemos que la obtención de un dominio en la red en las condiciones bajo estudio, desvinculado del destino que a él se asigne, no es una conducta típica. Cualquier finalidad que se le intente asignar queda dentro del marco de las meras suposiciones ya que no existen, ni posibilidad de obtener, evidencias que las confirmen mínimamente" (voto de los jueces Ballestero y Farah).

n. Juzgado en lo Correccional Nº1 de Bahía Blanca. "Faraoni, JM s/ corrupción mediante grooming". Causa Nº 1060/15. 1/6/2015.

Grooming. Tipicidad.

- Hechos

Se le imputaba a una persona haber contactado a un adolescente menor de edad a través de la red social Facebook.

- Decisión y fundamentos

El juzgado correccional lo condenó por el delito de *grooming,* de acuerdo a lo previsto en el art. 131 CP (BO 11/12/2013).

"[El grooming es] un delito doloso, autónomo, de peligro, en el que el legislador adelanta la barrera de protección tipificando actos preparatorios de un eventual abuso sexual, a fin de prevenir la comisión de estos delitos en perjuicio de los menores, dada su vulnerabilidad.

La acción típica consiste en contactar a un menor de 18 años a través de cualquier medio de comunicación tecnológica, es decir se trata de entablar una conexión personal a través de medios tecnológicos, un contacto 'virtual' como fase previa para la comisión de un delito que afecte la integridad sexual a través de un contacto corporal, aunque el delito subsiguiente podría cometerse sin este contacto directo.

Por eso, el contacto virtual con el menor no basta para configurar el delito sino que es necesaria la presencia de un elemento subjetivo ultraintencional distinto del dolo, un propósito subyacente del autor, que aparece redactado por la ley de la siguiente forma: '…con el propósito de cometer cualquier delito contra la integridad sexual de la misma' (cfme. Alejandro Tazza, El delito de grooming, La Ley del 7/03/14, 1 - La Ley 2014-B-521, AR/DOC/321/2014). Es decir que debe acreditarse la finalidad del autor de cometer cualquier delito de esta índole, pues el bien jurídico protegido es la integridad sexual, su reserva o libertad, como podrían ser abuso sexual simple, abuso sexual gravemente ultrajante, abuso sexual con penetración o violación, estupro, promoción o facilitación de la corrupción de menores, promoción o facilitación de la prostitución de menores, rufianería, pornografía infantil, exhibiciones obscenas, rapto.

Ahora bien, salvo que las conversaciones virtuales fueran muy explícitas, esta finalidad deberá inferirse, leyendo entre líneas las comunicaciones, teniendo en cuenta la

introducción de temas sexuales, con mayor o menor sutileza, y la propuesta de un encuentro personal y directo.

Claro está que como se trata de un delito de peligro, de un adelanto de la punibilidad hacia actos preparatorios, no es necesario que exista principio de ejecución de algún delito contra la integridad sexual para que se configure el injusto bajo estudio. Precisamente el ilícito previsto en el art. 131 del código de fondo en materia penal se consuma cuando se produzca el contacto virtual y pueda establecerse la ya mencionada finalidad de cometer un delito contra la integridad sexual, dado que se busca proteger la dignidad de los menores, como así su normal desarrollo psíquico y sexual, evitando los ataques que puedan comprometer dicho desarrollo.

Es preciso aclarar que no es necesario que el sujeto activo oculte o simule su identidad, o mienta en su edad al establecer el contacto, para que se configure el delito".

o. Tribunal Oral en lo Criminal de Necochea. "Fragosa, LN". Expte. T.C. Nº 4924-0244, 5/6/2013.

Grooming. Tipicidad.

▪ Hechos

Una persona fue imputada por corrupción de menores agravada por haber utilizado un nombre y fotografía falsos para contactar a una niña menor de edad por correo electrónico y Messenger. A su vez, le habría enviado archivos y mensajes con contenido sexual. El hecho ocurrió previo a la modificación legislativa que incluyó el *grooming* en el Código Penal.

▪ Decisión y fundamentos

El Tribunal Oral condenó al imputado a 10 años de prisión de conformidad con lo establecido en el art. 125, párrafos segundo y tercero, del Código Penal.

"[El delito de] 'grooming' [e]s un proceso sexual abusivo facilitado por el uso de las nuevas tecnologías que consiste en la interacción comunicacional de un adulto con un menor con fines sexuales y abusivos. Se lleva a cabo como proceso, a transitar evolutivamente.

El adulto interesado en conectar menores con interés sexual, en primer lugar debe conectar con un niño, lograr la relación empática, para luego llevar al menor a instancias donde el matiz sea sexual, que erotice la situación. En este tramo del proceso el objetivo del adulto es ganar la confianza del menor. Luego se busca sexualizar el vínculo con temáticas sexuales o intercambio de imágenes sexuales y/o pornográficas. Establecido esto, se intenta obtener la propia imagen del menor contactado, de características sexuales, donde el menor, por ejemplo, muestre su cuerpo desnudo.

[…]

Lejos de endilgar una conducta atípica al nombrado o de vulnerar el principio de legalidad como deslizara la Defensa al referirse al 'grooming', en el caso, esta actividad desplegada por [el imputado], subsume perfectamente en el tipo objetivo y subjetivo de la norma del art. 125, párrafos segundo y tercero, del Código Penal, pues ellos son los actos corruptores de la menor de 8 años de edad, L.M.

[E]s importante deslindar que el 'grooming' corruptor de la menor realizado por F., es un concepto compuesto por un abanico más o menos acotado de conductas realizadas por un sujeto contra un menor de edad.

En la exposición de motivos del proyecto de ley para penalizar específicamente el 'grooming', más allá que actualmente el grooming forme parte de actividades abusivas y corruptoras, como en el caso de autos […] se explica que el 'grooming' consiste en acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, al crearse una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.

Las redes sociales son un factor de riesgo para los menores, ya que no existe claridad respecto a la identidad de las personas con quienes conversan o se relacionan.

Etimológicamente, 'grooming' es una forma verbal de 'groom', vocablo cuyo significado alude a conductas de preparación o acicalamiento de algo, que en el ámbito de la pedofilia suele asociarse a toda acción que tenga por objetivo minar o socavar moral y psicológicamente a un niño, con el fin de conseguir su control a nivel emocional para un posterior abuso sexual. Respecto a su modus operandi, es una figura de 'acoso progresivo' que se verifica en etapas o períodos. Por lo mismo, suele denominársele también como 'acoso sexual infantil'.

Sus características podrían ser resumidas de la siguiente forma: (a) las conductas de childgrooming tienen como sujeto pasivo un menor de edad; (b) progresivamente el acercamiento se transforma en acoso intimidatorio; (c) se utilizan redes informáticas o telemáticas; (d) las conductas tienen contenido sexual, sea porque se busque obtener material pornográfico o bien porque se pretenda realizar un abuso sexual físico; (e) usualmente el agresor recurre a falsear su edad o identidad (ver al respecto Christian Scheechler Corona, 'El childgrooming en la legislación penal chilena: sobre los cambios al artículo 366 quáter del código penal introducidos por la ley nº 20526', publicado en la Revista chilena de derecho y ciencia política; Vol. 3, No. 1, 2012, p. 55-78)" (voto de la jueza Irigoyen Testa, al que adhirieron los jueces Juliano y Giménez).