

PRIMER CONGRESO DE JÓVENES PENALISTAS DE LA U.N.C.

-Problemas actuales de Derecho Penal y Criminología-

*DELITOS INFORMÁTICOS EN LA
LEGISLACIÓN ARGENTINA*

Autor:

Franco Daniel Pilnik Erramouspe

franco.pilnik@gmail.com

CÓRDOBA, Julio 2009

Delitos Informáticos: una aproximación a su conceptualización

Resulta difícil esbozar una definición de lo que se entiende por "Delito Informático", ya que, como fenómeno nuevo, aún no existe un consenso en cuanto a su conceptualización y, más aún, en lo referente a su ubicación y tipificación dentro de la doctrina y la legislación. El tema se centra en determinar si nos encontramos frente a un nuevo tipo de criminalidad que, necesariamente, requiera legislación, doctrina y jurisprudencia específica, o si al concepto clásico de delito debemos adicionarle cuestiones propias de esta nueva realidad, cual es la incorporación de la tecnología como herramienta que, por su particularidad, amerite un *aggiornamento* para una correcta subsunción del caso.

No caben dudas que, ante el crecimiento exponencial de los medios tecnológicos y la velocidad de la información, nos encontramos frente a un fenómeno que no debe escapar a la ciencia jurídica, y que merece un tratamiento particular. Pero, es a partir de un concepto claro y preciso de lo que se entienda por "Delito Informático", que podremos distinguir las acciones típicas, en las cuales se ha utilizado como medio comisivo un ordenador u otro medio tecnológico, o cuando dicho medio resulta el objeto del delito querido.

Una de las definiciones más completas del concepto buscado, fue dada por Hugo Daniel Carrión, quien sostiene que se pueden definir a los "Delitos Informáticos" como *"aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas"*¹.

A partir de esta definición, podemos identificar con claridad cuál es el "bien jurídico" tutelado en este tipo de delitos. Así, la información como bien intangible, ha cobrado en las últimas décadas un valor patrimonial sin precedentes, y no son pocas las empresas que basan su fortuna sólo en este tipo de bienes, los que hasta no hace mucho tiempo eran considerados intrascendentes.

Pero no son sólo las grandes corporaciones las que protegen su información. En la actualidad las personas individuales tienen almacenados en dispositivos electrónicos

¹ **CARRION, Hugo Daniel.** "Presupuestos para la incriminación del Hacking" -Revista Informática Jurídica- (en línea). Dirección URL: http://www.informatica-juridica.com/trabajos/presupuestos_para_la_incrimacion_del_hacking.asp#_ednref1 (consulta 10/06/09)

(computadoras personales, *notebooks*, *blackberries*, etc.) datos de suma importancia, aquellos que hacen a su intimidad y negocios, y que merecen ser protegidos. Esta situación, era impensada al momento de la redacción de nuestro Código Penal (C.P.).

Es entonces esa información, en el sentido más amplio, la que se traduce en datos con sentido patrimonial, -además de íntimos-, como son las fotografías, bases de datos, asientos contables, sitios *web*, etc.. Ello implica, necesariamente, que los mismos deben ser protegidos, tanto en su lugar de almacenamiento, como durante su transferencia o reproducción. Piénsese que el Estado no puede quedar ajeno y desconocer que estos bienes conforman en la actualidad, utilidades sin las cuales no se puede pensar en un mundo modernizado tecnológicamente.

Respecto de quien es el “sujeto activo” en estos delitos, nos encontramos con una de las notas más características de este tipo de delincuencia. Aquí aparece una singular similitud con los llamados “*delitos de cuello blanco*”², donde el delincuente informático posee un alto nivel de conocimientos técnicos sin los cuales se le haría imposible desarrollar su actividad. No en todos los casos esos conocimientos son adquiridos en Universidades o Institutos, sino que, muchas veces provienen de largas horas frente a ordenadores personales o de información que circula por la red de Internet, o es publicada en foros *on line*³, pero seguramente se requerirá de un estudio previo y alta capacidad de comprensión.

Este tipo de delincuente, además de poseer por lo general un *status* socio-económico medio o elevado, no necesita exponerse físicamente para cometer el delito, ya que incluso puede hacerlo desde la comodidad de su casa y a miles de kilómetros del lugar del hecho. En algunos casos, como los de intromisión en sistemas altamente protegidos, puede no buscar un rédito económico o causar perjuicio, sino simplemente demostrar que se es capaz de vulnerar sistemas supuestamente impenetrables. Casi que podría inferirse que el fin perseguido es mejorar la imagen ante sí mismo y sus pares, y no verdaderamente causar un daño o apropiarse de algo ajeno.

En relación al “sujeto pasivo”, demás está decir que no se trata del dispositivo sobre el que se realiza la operación ilegal, sino el “titular” del derecho contenido en dicho dispositivo, y sobre el cual recae la acción dañina. En un comienzo fueron los bancos a través de transacciones en línea los que sufrieron este tipo de atentados. Luego, incluso el propio Estado fue víctima de delincuentes informáticos. Recuérdese el caso de intromisión al sitio *web* de la Corte Suprema de Justicia de la Nación en el año 1998. Empero, en la actualidad,

² Concepto introducido por el criminólogo norteamericano Edwin Sutherland en el año 1943.

³ **Foro (Internet):** “Por lo general los foros en Internet existen como un complemento a un sitio *web* invitando a los usuarios a discutir o compartir información relevante a la temática del sitio, en discusión libre e informal, con lo cual se llega a formar una *comunidad* en torno a un interés común” (en línea) Dirección URL:[http://es.wikipedia.org/wiki/Foro_\(Internet\)](http://es.wikipedia.org/wiki/Foro_(Internet)) -(consulta 12/07/09)

cualquier persona que use una computadora personal, o cualquier dispositivo capaz de almacenar y transferir datos, puede ser objeto de este tipo de delincuencia.

Legislación Nacional

En nuestro país, no existía una regulación específica en la materia, y no fue sino hasta junio del año 2008 -cuando se sancionó la Ley Nro. 26.388-, que comenzamos a ser uno de los Estados con normativa definida en el campo de los “Delitos Informáticos”. En este caso, el legislador no optó por generar un capítulo destinado a la problemática que nos atañe. Por el contrario, creó nuevas normas diseminadas por el Código Penal, determinando nuevos tipos penales, o actualizando otros ya en uso.

No deja de ser una cuestión importante el haber agregado a los últimos párrafos del Art. Nro. 77 del C.P., algunos términos que, por su especificidad en la materia, podrían generar dudas sobre su aplicación, sentido o alcance. Así es que, se ampliaron conceptos clásicos para abarcar situaciones actuales. Ahora un “documento” puede estar contenido en cualquier soporte, incluido obviamente el electrónico. Los términos “firma” y “suscripción” comprenden: a) la firma digital; y b) la creación de una firma digital, o firmar digitalmente. Así como “instrumento privado” y “certificado” comprenden al documento digital firmado digitalmente. Lo apuntado anteriormente tiene estrecha vinculación con la Ley Nro. 25.506, llamada de “Firma Digital”, ya aprobada hace algunos años. Esta Ley creó un marco de avanzada en la materia, ampliando la posibilidad de generar operaciones mucho más seguras y a distancia, pudiéndose comprobar la identidad de los firmantes mediante un sofisticado sistema de certificación, pero que en caso de comisión de algún ilícito, no encontraban su correlato en material penal.

Ya en la parte especial del Código, y dentro del Título de los “Delitos contra la Integridad Sexual”, se modificó el Art. Nro. 128, con la idea de combatir el grave flagelo de la *pornografía infantil* que se extiende por toda la red generando un negocio millonario. Se ha dicho 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 C.P. contemple esta nueva modalidad delictual, sobre todo para cumplir con los compromisos internacionales que la Argentina ha adoptado.

Nuestro país, a través del Art. Nro. 75 inc. 22 de la C.N., ha incorporado con rango constitucional la “*Convención sobre los Derechos del Niño*” de Naciones Unidas, que prevé en su Art. Nro. 34, la protección al menor “*contra todas las formas de explotación y abusos sexuales*”. También, a través de la Ley Nro. 25.763 aprobó el Protocolo relativo a la “venta de

niños”, “prostitución infantil” y la “utilización de los niños en la pornografía”, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño, y que dispone que “*Los Estados Parte prohibirán la venta de niños, la prostitución infantil y la utilización de niños en pornografía infantil*”.

El nuevo Art. Nro. 128 del C.P., amén de incluir nuevas conductas típicas, en lo que a este trabajo interesa, agrega la expresión “*por cualquier medio*”, como modalidad comisiva. Ello apunta, definitivamente, a la transmisión de imágenes pornográficas que incluyen a menores de 18 años de edad. Se refiere no sólo a Internet como canal principal, sino también, -como ha sucedido en algunos casos resonantes de los últimos tiempos entre alumnos de colegios secundarios-, a la transmisión de fotografías o videos pornográficos utilizando la tecnología *bluetooth*⁴ (sistema que poseen en la actualidad la mayoría de los teléfonos móviles), o el envío del material de un celular a otro, a través del sistema de *mensaje multimedia* (mms)⁵.

También se sustituyó el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: “*Violación de Secretos y de la Privacidad.*” De esta manera, el nuevo Art. Nro. 153, castiga la interceptación o captación de comunicaciones electrónicas o telecomunicaciones. Se utiliza, con dicha expresión, una terminología amplia que se puede aplicar tanto a los correos electrónicos, como a los mensajes enviados desde o hacia cualquier dispositivo móvil (teléfono celular, *palm*, *blackberry*, etc.), como cualquier otro que pueda surgir en el futuro.

También se utilizó la locución “*indebidamente*” para que no queden dudas del carácter doloso que deber tener el autor del delito. Si bien esta cuestión ya había sido resuelta por la jurisprudencia con el texto anterior de la norma, en el caso del periodista Jorge Lanata⁶, donde se equiparaba al *email* con la correspondencia tradicional, no fueron pocas las críticas que se suscitaron, aduciendo que se trataba de una interpretación analógica de la ley penal.

⁴ **Bluetooth:** “*Bluetooth, es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). Es posible interconectar teléfonos celulares, computadoras, notebooks, palms, etc debido al avance de la tecnología en este campo, cada vez más dispositivos electrónicos tienen esta tecnología, que fue conocida en nuestro país por la venta*” (en línea). **Dirección URL:** <http://es.wikipedia.org/wiki/Bluetooth> (consulta: 02/07/09)

⁵ **Sistema de Mensajería Multimedia:** “*Multimedia Messaging System (MMS) o sistema de mensajería multimedia es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos o cualquier otro contenido disponible en el futuro. La mensajería multimedia nos permite el envío de estos contenidos además a cuentas de correo electrónico, ampliando las posibilidades de la comunicación móvil, pudiendo publicar nuestras fotografías digitales o actuar en weblogs sin mediación de un ordenador. El límite de cada mensaje multimedia suele ser de 100 o 300 KB, dependiendo de cada móvil, si bien ese límite lo definen el operador o las características del terminal y no el protocolo*”. (en línea) **Dirección URL:** http://es.wikipedia.org/wiki/Multimedia_Messaging_System (consulta: 02/07/09)

⁶ Lanata, Jorge - Cámara Nacional De Apelaciones En Lo Criminal Y Correccional, Sala VI, (C. Nac. Crim. y Corr., sala 6ª, 04/03/1999 - Lanata, Jorge). JA 1999-III-237.

Pero lo que sí se ha presentado como un novedoso *leading case*, es la posibilidad de que los padres, apelando al interés superior del menor, puedan abrir los correos electrónicos de los hijos en los casos de sospechas de que pudieran ser víctimas de abusadores sexuales⁷.

El nuevo Art. Nro. 153bis, pune el acceso a un sistema o dato informático, comúnmente denominado “*Hacking*” (aunque se ha distinguido el “*hacking*” como una intromisión sin fines de causar daño, del “*cracking*” que es la que busca causar perjuicio), si el mismo se ha concretado a través de un medio informático, es decir, la intromisión sin autorización a un sistema restringido, o bien excediendo la que ya se posee.

Se ha definido al “*Hacker*” como un informático que utiliza técnicas de penetración no programadas para acceder a un sistema informático con los más diversos fines: satisfacer su curiosidad, superar los controles, probar la vulnerabilidad del sistema para mejorar su seguridad, sustraer, modificar, dañar, o eliminar información, y cuyas motivaciones también responden a los más variados intereses (ánimo de lucro, posturas ideológicas anarquistas, avidez de conocimientos, orgullo, propaganda política, etc.)⁸.

Esta figura es de carácter subsidiario a que no se configure un delito más severamente penado, agravándose en el caso que el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal, de un proveedor de servicios públicos, o de servicios financieros. Es que la idea del legislador fue la de perseguir a quienes ingresaran a un sistema protegido, violando de esa manera la privacidad y confidencialidad de una persona o empresa, pero si, con ese acceso se produce un daño u otro delito, la figura queda desplazada por el carácter subsidiario antes comentado. El acceso generalmente suele ser remoto y hasta por programas automáticos destinados a tal fin para recoger información de los usuarios.

La publicación de una comunicación electrónica es penada por el Art. Nro. 155 C.P. Esta norma utiliza la expresión “*comunicación electrónica*” para que pueda ser aplicada no sólo a los correos electrónicos, sino a cualquier comunicación digital, como son actualmente los mensajes de texto de la telefonía móvil, *chats*, mensajes a través de redes sociales como *Facebook*, etc. En estos casos se trata de hacer público un mensaje o conversación entre una o varias personas. Se ha dicho que los medios de prensa estuvieron detrás de la sanción inicial

⁷ Clarín, “Es legal que un padre espíe la casilla de correo de su hijo”, diario del 30/06/09. Dirección URL: <http://www.clarin.com/diario/2009/06/30/sociedad/s-01949230.htm> (en línea) (consulta: 30/06/09)

⁸ Op. Cit. Carrion

de esta norma, a raíz de las violaciones de correo electrónico ocurridas en el año 2006 a varios periodistas⁹.

Conforme quedó redactado el Art. Nro. 157bis, queda punido el *acceso a un banco de datos* (inc. 1º), *revelación de información* (inc. 2º) y *alteración de datos* (inc. 3º). Así, el inc. 1º castiga el ingreso por cualquier medio a un banco de datos personales. Aquí se aplica lo dicho sobre el “*Hacking*” en el comentario del Art. Nro. 153bis, donde también se dijo que esta última figura tenía un carácter subsidiario para que no resultare un delito más severamente penado, como es el caso de la intromisión de la que estamos hablando. En ambos casos la acción típica es: “*acceder a sabiendas e ilegítimamente*” por cualquier medio o de cualquier forma. Pero si ese acceso está dirigido a una base de datos personales, el hecho recae sobre esta figura con pena mayor.

En relación al inc. 2º, se castiga la “revelación de información registrada en un banco de datos personales y cuyo secreto se estuviere obligado a guardar”. Piénsese que en la actualidad existen bases de datos con información personal que son de vital importancia y que hacen a la vida, intimidad, y negocios de las personas, y que su publicación indebida puede causar un grave perjuicio para el mismo. Cabe destacar que la información puede estar también contenida en una “archivo” como reza la norma, y no solamente en una “base de datos”.

Finalmente, el inc. 3º reprime la inserción de datos en un archivo de datos personales. Aquí hubo una fusión entre el Art. Nro. 117bis inc. 1º (hoy derogado justamente por la Ley Nro. 26.388), y el inc. 3º de la norma en cuestión. De la unificación de ambos artículos, se ha buscado la protección no solo del honor de las personas, sino también de su actividad comercial. Resultaría un perjuicio enorme, por ejemplo, que alguien sea ingresado indebidamente a algún sistema de servicio de situación financiera como Seven o Veraz¹⁰, con una calificación negativa de deudor incobrable.

Se agregó también el inc. 16 al Art. Nro. 173 del C.P., estableciendo un nuevo tipo de estafa o fraude. Se incluyó esta figura dentro de las que corresponden a “*defraudaciones*”, dando fin a la discusión acerca de qué tipo de delito contra la propiedad se trata. Tal como lo ha definido el autor Pablo A. Palazzi¹¹, la acción típica consiste en defraudar mediante la manipulación en un ordenador u otro artilugio informático, de modo tal que altere el normal

⁹ Clarín, “Espían y roban correos electrónicos de un juez y de un periodista de Clarín”, diario del 11/05/2006. Dirección URL: <http://www.clarin.com/diario/2006/05/11/elpais/p-01001.htm> (en línea). (consulta: 05/07/09)

¹⁰ Dirección URL: <http://www.veraz.com.ar/> ó <http://www.seven.com.ar/> (en línea)

¹¹ PALAZZI Pablo A., Los Delitos Informáticos en el Código Penal – Análisis de la ley 26.388. Abeledo Perrot, Buenos Aires, 2009, pág. 179

funcionamiento de un sistema informático o la transmisión de datos, y si alguno de estos dos requisitos faltara, no se darían los elementos requeridos por el tipo penal. La idea central aquí, es que el sistema tiene un funcionamiento normal y predecible, y el delincuente, a sabiendas de cómo funciona el mismo, lo “*engaña*” mediante diferentes técnicas para lograr un beneficio patrimonial.

Por último, se tipificó el “*daño informático*”, a través de los nuevos Arts. Nros. 183 segundo párrafo y 184, incs. 5° y 6° C.P. En el primer caso, la acción típica es la de “alterar”, “destruir” o “inutilizar” los datos contenidos en un ordenador (ya sea una computadora personal, servidor, o cualquier otro medio de almacenamiento de sistemas informáticos). Aquí, -como señala el citado autor Pablo Palazzi¹²- nos encontramos ante tres conductas: a) la de “alterar”, que no significa “borrar”, pero sí generar una modificación tal que haga que el archivo no pueda volver a ser utilizado; b) “destruir”, que implica producir un borrado total de la información, de modo tal que no pueda ser recuperada a través del mismo sistema operativo a través de su procedimiento de guardado en la “papeleras de reciclaje”; c) e “inutilizar”, que implica que si bien el archivo sigue existiendo, no puede ser utilizado para el fin que fue creado.

También explica que, en nada cambia la tipicidad, que el usuario haya tenido un *backup* o copia de respaldo de la información, ya que el hecho de tener que restaurar lo borrado requiere un esfuerzo que ya implica un daño.

Este tipo de delitos se producen principalmente por la intromisión de un *virus* dentro del ordenador, que nos es más que un programa que ejecuta una acción dañina. El daño a que da lugar este delito puede recaer sobre “datos”, “documentos”, “programas” o “sistemas informáticos”. Esta es la principal modificación que requería nuestro código penal. La ausencia en cuanto a la referencia de tales objetos en la descripción del Art. Nro. 183 CP llevó en numerosos casos a concluir que la destrucción de un archivo digital resultaba atípica.

Una de las cuestiones más novedosas en relación al Art. antes mencionado, está referido a la persecución de quien “vendiere”, “distribuyere”, “hiciera circular” o “introdujere en un sistema informático”, cualquier programa destinado a causar daños. Es decir que, no solamente se pena a quien causa el mismo, sino también a aquellos que tienen a su cargo la cadena de distribución y que están poniendo en el comercio o en circulación programas susceptibles de provocar daño. Finalmente, el delito se agrava si el daño se produce sobre “datos”, “documentos”, “programas” o “sistemas informáticos públicos”, o bien si se ha ejecutado el hecho sobre sistemas informáticos destinados a la prestación de servicios de

¹² *Ibíd.* Pág. 187

salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Infracciones Penales a la Ley de Propiedad Intelectual a través de medios digitales masivos

La creciente masificación de la red Internet y dispositivos digitales que permiten el almacenamiento y transmisión de datos a gran velocidad, ha generado una revolución en el consumo de obras intelectuales protegidas por la Ley Nro. 11.723 (y su modificación por la Ley Nro. 25.036 con la que se brinda protección legal al *software*).

Hoy en día, -y en líneas generales-, las personas tienen a su alcance una computadora personal, *notebook*, *Iphone*, o teléfono móvil, elementos todos que requieren de un *software* para funcionar. Esos dispositivos también son usados para escuchar música, o bien ver películas o series, incluso antes de que los mismos se estrenen en el cine o televisión. El problema radica en que, son pocas las personas que pagan por la utilización de todos estos beneficios. Salvo en el caso de las computadoras portátiles, -que ya vienen con el sistema operativo preinstalado de fábrica-, es común que quien acude a un comercio a comprar un ordenador de escritorio, le sea ofrecido gratuitamente (o a muy bajo costo), la instalación del mismo (Windows en el 99% de los casos), el paquete de procesador de texto, y demás herramientas de MS Office, antivirus, etc. Ni que hablar de la descarga y uso de música protegida, que se realiza a través de archivos comprimidos mediante el sistema MP3, y que pueden ser utilizados tanto en ordenadores, teléfono móviles, como en reproductores portátiles.

Así es que, cualquier ciudadano tiene al alcance de su mano tecnología suficiente como para hacer uso de obras con Copyright. La cuestión de fondo es que son muy escasas las personas que pagan por estas instalaciones, o si lo hacen, es a muy bajo costo en relación al precio original. Nada más con abrir cualquier matutino local, uno puede encontrar ofrecimientos de CDs de música, películas y *software* a un precio menor que un menú de casa de comidas rápidas. Pero también puede decirse que son pocos los que saben que deben pagar por ello. Y esto es a partir de que no existe en nuestro país una conciencia generalizada de reconocimiento a los derechos de autor.

Nuestra Ley de Propiedad Intelectual castiga con la misma pena del Art. Nro. 172 del C.P., a quienes “reproducen”, “venden” o “editan” una obra sin consentimiento de su autor. Pero, ¿por qué son tan pocos los casos que se ventilan en nuestro Tribunales, siendo que, como ya se dijo, las violaciones a estos derechos son flagrantes? Una de las cuestiones, como

me referí anteriormente, es la *falta de cultura* por el respeto a la obra intelectual. Cualquiera sabe que robar, matar o violar, es una *infracción*, pero quienes consiguen música para escuchar con su celular, ni siquiera imaginan que se trata de un “delito”. Tan es así, que hace algún tiempo, una empresa proveedora de servicios de Internet (ISP) publicitaba que, contratándolos, se podía bajar a la mayor velocidad toda la música que uno quisiera. Luego de varias quejas por parte de las compañías discográficas, se aclaró que era solo de los sitios legales y mediante el pago correspondiente. Pero ello es muestra de cómo no está totalmente arraigada la idea de que, para consumir obras protegidas, se debe pagar por ellas.

Es a partir del gran esfuerzo realizado por los titulares de estos derechos (compañías cinematográficas, disqueras, etc.) que se persigue y castiga a los infractores. Hace pocos días se publicó una noticia¹³ acerca de que sólo en el primer trimestre del año 2009, se habían procesado a 18 personas consideradas responsables de defraudación contra la propiedad intelectual. Ello amén de haberse realizado numerosos allanamientos y secuestro de PCs con “programas piratas”, CDs y DVDs. Todo esto tuvo como punto de partida las denuncias realizadas por BSA¹⁴, quienes vienen realizando ingentes esfuerzos acerca de este tema. Es decir que, si bien se trata de delitos perseguibles de oficio, la mayoría de los casos que se investigan son a partir de la actuación privada.

También se ha dicho que uno de los problemas que genera el fenómeno de la piratería, es el altísimo costo del *software*, principalmente para el usuario doméstico ya que, los precios deben ser abonados en dólares. Por ello, el Estado Argentino, a través de la Ley de Promoción de la Industria del Software” Nro. 25.922, no solo ha incentivado a los desarrolladores locales de *software*, sino que ha posibilitado el acceso a programas a un precio más accesibles para el consumidor de este tipo de productos. Esto es expresión de tres cuestiones fundamentales: a) la toma de conciencia en cuanto a la necesidad de proteger los derechos del autor; b) evitar que se menoscabe la producción intelectual; y, c) favorecer la accesibilidad de todos los usuarios a dichos productos. De esta manera, puede observarse un progreso en cuanto al tratamiento de la problemática específica.

Problemas relativos a la Jurisdicción y Competencia

¹³ Diario Comercio y Justicia, edición del día miércoles primero de julio de dos mil nueve, pág. 06

¹⁴ Business Software Alliance (BSA) es una organización sin fines de lucro creada para promover los objetivos de la industria del software y proteger los derechos de propiedad intelectual de los proveedores de software. **(en línea) Dirección URL:** http://www.bsa.org/country.aspx?sc_lang=es-AR

La cuestión relativa a la jurisdicción para perseguir y penar los delitos informáticos se presenta como un gran desafío para los operadores del derecho. Es que, dada la complejidad con que se suelen dar este tipo de maniobras, no siempre resulta fácil determinar el campo de acción sobre los mismos. Imaginemos que un ciudadano de origen chino, situado en Alemania, usando servidores que se encuentran alojados en Australia, comete un fraude informático contra un banco radicado en Argentina. O imaginemos también la situación en la que alguien crea un virus informático en Chile, pero causa daños en nuestro país. ¿No debemos acaso preguntarnos, quién es el Juez Competente para el caso, y aún más, qué legislación corresponde aplicar? Nuestro código penal recepta el principio de “*territorialidad*” (Art. Nro. 1 C.P.), pero como hemos visto anteriormente, estas cuestiones exceden las soluciones dadas para el delito común, ya que existe una “*multiterritorialidad delictiva*”.

En relación con esta cuestión, a nivel internacional ocurrieron casos paradigmáticos. Uno de los primeros fue el denominado *Gutnick v. Dow Jones & Co. Inc.*¹⁵ Allí, un empresario australiano de nombre Joseph Gutnick decide demandar por difamación en los tribunales de su domicilio a la compañía americana de medios *Dow Jones & Co.*, ya que en octubre de 2000 la revista *Barrons Digest* (publicación de *Dow Jones*) saca a la luz un material, tanto en su versión en papel como en su portal, que atribuye algunas características de fraude y de lavado de dinero al señor Gutnick dentro del territorio de Australia. Esto también fue publicado en el prestigioso *Wall Street Journal*. El Tribunal Superior de Victoria (*Victoria Supreme Court*) —lugar de residencia del Sr. Gutnick— decide conocer de la controversia, señalando en su resolución que los habitantes de dicha región tuvieron acceso y pudieron leer el artículo en ambos medios informativos. La empresa Down Jones se defendió y apeló la decisión del juez australiano, argumentado, principalmente, la aplicación del “principio de territorialidad”, es decir, la ley penal aplicable donde tuvo lugar la comisión del hecho, esto es, el lugar de la difamación. Según la defensa, la misma se habría llevado a cabo en territorio norteamericano, que es donde se encuentran situados los servidores de Down Jones. El caso se resolvió a través de una negociación, pero resulta importante para graficar la problemática planteada ya que, si bien los servidores están situados en un país, cualquier ciudadano del mundo con conexión a Internet podía acceder a ellos.

Son éstas, así como otras cuestiones técnicas, las que hacen difícil encontrar una solución en casos como el apuntado, por lo que se deberá estudiar cada uno de ellos y, por una cuestión de economía procesal, tendrá que entender el juez que tenga más a mano la posibilidad de generar las pruebas, y donde el imputado pueda realizar mejor su defensa.

¹⁵ Ejemplo publicado por: **ABOSO Gustavo Eduardo - ZAPATA María Florencia**, *Cibercriminalidad y Derecho Penal*. Buenos Aires, B de f, 2006, pág. 32

Responsabilidad de los ISP

Los ISP (*Internet Service Providers*) son las empresas que brindan el servicio que nos posibilita navegar por Internet (en nuestro país: Arnet o Fibertel, por ejemplo), y es a través de su prestación que se cometen, justamente, algunos “delitos en línea”. El tema se centra en delimitar cuál es su “*responsabilidad*” por el uso que hagan los usuarios con el servicio que se les presta. Como ya se dijo, mucha gente “descarga” música o películas que luego comparte con otros navegantes, lo que constituye una clara violación a la ley de Propiedad Intelectual. Otros pueden utilizar el servicio para “intercambiar fotografías con contenido sexual que incluyan a menores”, “esparcir un virus informático” o “ingresar a un sistema restringido”. Corresponde, entonces, determinar cuál es la responsabilidad de las empresas que intermedian en el servicio de conexión a Internet, para el caso en que se cometa un delito.

Resulta útil hacer una diferenciación entre los distintos “actores” que aparecen en la navegación *web*, a los fines de precisar qué roles cumplen cada uno de ellos en lo que a responsabilidades vinculadas con el delito se refiere. Así, nos encontramos: a) como ya se dijo anteriormente, con los ISP, que nos proveen de la conexión para navegar por Internet; b) luego tenemos los Servicios de *Hosting* (HSP= *Hosting Service Providers*), sobre cuyos servidores se alojan las páginas *web*; c) a su vez están los proveedores de contenidos o creadores de los sitios, cuyas páginas se almacenan en los HSP y a cuyo contenido accedemos a través de los ISP; y d) finalmente están los usuarios de los distintos servicios. Es así que, si uno de estos últimos comete un delito por Internet, debemos precisar qué responsabilidad le cabe a cada uno de estos actores.

Ejemplificando lo expresado anteriormente, tomemos el caso de una persona que envía un *e-mail* a otra, utilizando cuentas por ejemplo de Hotmail, y en ese correo adjunta imágenes de menores teniendo sexo. No caben dudas de que aquí nos encontramos ante un hecho atrapado en el nuevo Art. Nro. 128 del C.P. No obstante, resulta dificultoso determinar las responsabilidades tanto de Microsoft, por ser la proveedora de *e-mails* gratuitos Hotmail, como la ISP a través de cuya conexión se transmitieron los datos. Esto así, porque por día se envían y reciben millones de correos electrónicos a través de Hotmail, mucho de los cuales llevan adjuntos fotografías. Este fenómeno hace casi imposible que la empresa pueda determinar cuáles de ellas tienen contenido prohibido. Control que, además, atentaría contra la privacidad del correo privado. Para resolver esto, la empresa, a lo sumo, podría incluir algún servicio automático que detectase si el archivo que contiene la imagen es, por ejemplo, de contenido pedófilo. Pero, para que ello sea posible, el archivo que contiene la imagen debería

tener incorporada una descripción, que es lo que la máquina podría detectar. La solución es más sencilla si se trata de “virus informáticos”, ya que son programas que, por su estructura, pueden ser detectados por los sistemas previstos, aunque no son infalibles como se ha visto.

Técnicamente es casi imposible controlar los miles de millones de *bits* de información que circulan por la red en un solo día. Lo mismo sucede con la proveedora de servicio de conexión, en cuanto al filtrado y detección de delitos cometidos a través de su servicio. Aunque, a los fines de la *protección* de los *derechos intelectuales*, se han tomado algunas medidas en cuanto al filtrado de paquetes de información transmitida, cuando se trata de los sistemas de intercambio de archivos *p2p* (*peer to peer*), que tan basta difusión tienen en la *web*.

Distinto es el caso de los proveedores de contenido de una *website*. Quien desarrolla o administra un sitio cuyo contenido es ilícito, debe responder por las infracciones cometidas en ellos. La solución es sencilla, si quien administra el sitio y el proveedor de lo que allí se publica se trata de la misma persona o empresa. Pero no todo el contenido de las *websites* es producido por su creador, sino que, como en el caso de los foros, son los usuarios los que aportan lo que se publica. Un ejemplo de ello es lo que ha sucedido en nuestro país con el caso llamado “*Jujuy.com*”¹⁶, donde una persona ingresó a www.jujuy.com y publicó declaraciones injuriosas sobre un supuesto adulterio. En ese caso, se accionó contra los creadores del sitio, por no haber controlado el contenido de lo que se publicaba. Queda claro, entonces, que existe responsabilidad de quien no controla lo que se publica o, en su caso, de quien siendo notificado de que existe material delictivo “*colgado*” en un servidor de Internet, no lo elimina.

Algunas Conclusiones

Luego de este breve análisis sobre algunas cuestiones relacionadas con la Informática y el Derecho Penal, es probable que nos hayan quedado más dudas que certezas. Es que, los nuevos sistemas digitales y la velocidad de la información se desplazan de manera tan rápida que se hace difícil tipificar y subsumir todas las variantes delictivas que con ellas se pueden cometer. Tan es así que, ni siquiera los autores se ponen de acuerdo sobre el concepto de “Delitos Informáticos”, y si realmente se pueden escindir de los delitos comunes como una rama especial. Ello, sumado a la complejidad con que se presenta este tipo de “delincuencia” y la “multiterritorialidad” de jurisdicciones, no hacen más que generar un terreno propicio

¹⁶ Superior Tribunal de Justicia de la Provincia de Jujuy S. M. y L. E. M. de M. c. Jujuy Digital y/o Jujuy Com. y O. L. Publicado en: LLNOA 2006 (febrero), 31

para que muchos se aprovechen de lo que común y coloquialmente llaman “fallas del sistema”.

Nuestro país ha dado un gran paso al sancionar la Ley Nro. 26.388 y, con ella, ha armonizado nuestra legislación con la de varios de los miembros regionales del Mercosur. Con esta nueva Ley se podrán perseguir y penar muchas conductas que, ante el vacío legal, quedaban impunes y generaban cuantiosas pérdidas económicas. Aún así, todavía resta regular la situación de todos los actores que aparecen involucrados en la interacción electrónica, ya que es a partir de una correcta distinción de qué roles cumplen cada uno, que se podrán delimitar responsabilidades.

En cuanto a las infracciones a la Ley de Propiedad Intelectual por “medios digitales masivos”, si bien existe en nuestro país un gran consumo de mercadería “pirata”, es a través del esfuerzo de muchas instituciones privadas, la toma de conciencia por parte del Estado, y la reacción del consumidor en busca de un producto más seguro, que se va logrando revertir esta la tendencia.

En definitiva, esta nueva problemática se presenta como un gran desafío para todos los operadores del derecho, quienes deberemos adaptarnos a las nuevas situaciones tecnológicas e intentar, utilizando las herramientas existentes, brindar un mejor servicio de justicia, tanto en el ejercicio profesional independiente como dentro del sistema del Poder Judicial.

Franco Daniel Pilnik Erramouspe

D.N.I. Nro: 26.313.280

franco.pilnik@gmail.com

BIBLIOGRAFÍA

1. **ABOSO, Gustavo Eduardo – ZAPATA, María Florencia**, *Cibercriminalidad y Derecho Penal*. **B de f, Buenos Aires, 2006.**
2. **CABANELLAS DE LAS CUEVAS, Guillermo**, *Régimen jurídico de los conocimientos técnicos*. **Heliasta, Buenos Aires, 1984.**
3. **DONNA, Edgardo**, *Derecho penal. Parte especial*. **Rubiznal- Culzoni, Santa Fe, 2001.**
4. **NUÑEZ, Ricardo C.**, *Manual de derecho penal. Parte general*. **Lerner, Córdoba, 1977.**
5. **PALAZZI, Pablo A.**, *Delitos Informáticos. Ad Hoc*, **Buenos Aires, 2000.**
- *Delitos Informáticos en el Código Penal – Análisis de la ley 26.388*. **Abeledo Perrot, Buenos Aires, 2009.**
6. **RIQUERT, Marcelo A.**, *Protección penal de la intimidad en el espacio virtual*. **Ediar, Buenos Aires, 2003.**
7. **TRABALLINI DE AZCONA, Mónica**, *Delitos contra la propiedad intelectual. Las disposiciones penales de la ley 11.723 y la copia privada*. **Mediterránea, Derecho Penal Contemporáneo, Serie Azul, vol. 5, 2004.**
8. **VILLALBA, Carlos – LIPSZYC, Delia**, *El derecho de autor en Argentina*. **La Ley, Buenos Aires, 2001.**