

Actualidad en derecho penal informático

Protección penal de las bases de datos

Por Pablo A. Palazzi

SUMARIO: I. Introducción.- II. Base de datos: a) *La protección penal del derecho a la intimidad*: 1. Revelar a terceros información registrada en un banco de datos personales; 2. Acceso ilegítimo a un sistema informático; b) *La protección penal del derecho del compilador*: 1. El caso "Nosis v. Axesor"; 2. El caso "Reidman"

I. INTRODUCCIÓN

En esta oportunidad abordaremos el comentario de tres casos penales relacionados con bases de datos. El primero trata del acceso ilegítimo a bases de datos y a correos electrónicos. La sociedad de la información en que vivimos nos obliga a dejar información personal en ordenadores y bases de datos. Cada vez con mayor frecuencia éstos resultan más vulnerables. Por eso es importante amparar la seguridad y privacidad de la información contenida en ordenadores y bancos de datos no sólo civilmente, sino también a través de normas que brinden una efectiva protección y disuasión. Nos referimos a las normas penales. Esto no es ninguna novedad, pues ya hace tiempo la insuficiencia del amparo civil frente a la necesidad de protección penal de la privacidad era denunciada por uno de nuestros más conocidos civilistas (1).

Los dos restantes fallos enfocan la protección penal de las bases de datos como bienes intangibles de la empresa, esto es, la protección de su contenido por su valor económico. La producción y obtención de información tiene un costo. Se invierte tanto dinero como tiempo en su obtención. Esto genera un interés en poder amparar jurídicamente las bases de datos que tienen un alto valor comercial.

II. BASES DE DATOS

a) *La protección penal del derecho a la intimidad*

En el caso "Feldman" (2) se discutía la significación penal de dos formas muy comunes de atacar la privacidad: la

primera consistió en la apropiación de una base de datos de correos electrónicos y luego su difusión en un sitio web. La segunda consistió en el acceso a tres cuentas de correo electrónico de otros usuarios, su manipulación y su alteración. Ambos hechos se investigaron en la misma causa.

El tribunal concluyó que el primer hecho podría ser considerado un delito penal. En relación con el segundo fue muy claro en cuanto a que la conducta era atípica.

1.- Revelar a terceros información registrada en un banco de datos personales

Como explicamos, se investigaba la apropiación de una base de datos de correos electrónicos y su difusión a través de una página en internet. En concreto, la base de datos de usuarios de uno de los proveedores de acceso a internet más importantes del país (Fiberte! S.A.) fue publicada en la página web www.infohack.org, propiedad del imputado Feldman. El imputado fue sobreseído en primera instancia de los delitos contemplados en los arts. 117 bis, 156 y 157 bis CPen.

La Cámara del Crimen revocó ese fallo. La decisión se limita a señalar que el hecho en cuestión estaba probado y que la explicación del imputado perdía "eficacia ante la declaración de los expertos, en el sentido de que sus expresiones, si bien son técnicamente posibles, resultan ... poco creíbles dado que la información encontrada en el portal de su propiedad es... muy trabajada y no se corresponde con información subida por error o de casualidad sin que nadie lo advierta". Luego el fallo agrega: "Sin perjuicio de ello, habrá de profundizarse la investigación a

(1) Borda, Guillermo, "Una ley estéril", ED 67-581 (1976). El autor, al comentar la reforma del Código Civil que introdujo el art. 1071 bis, sostuvo: "La turbación de la intimidad debería ser incriminada como delito. Sólo así es posible concebir la esperanza de que la protección legal sea efectiva".

(2) Caso "Feldman, Adrián y otro - art. 117 bis CPen.", de la C. Nac. Crim. y Corr., sala 7ª, del 20/10/2004.

efectos de deslindar responsabilidades en la propia empresa denunciante con relación a quién habría proporcionado a Feldman dichos datos".

La conclusión del tribunal nos parece acertada. Entendemos que el tribunal se está refiriendo al art. 157 bis párr. 2º CPen. ("Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley"). Esta conclusión del tribunal lleva implícito el hecho de considerar que el correo electrónico es un dato personal (3) y que publicar la base de datos personales completa en Internet equivale a difundirla.

La lógica nos dice que, previo a su publicación en internet, alguien debió acceder al banco de datos (4), y por ello el tribunal ordena profundizar la investigación (5). Lo que suele suceder frecuentemente es que el denunciado se encuentra en poder de datos personales y no puede explicar cómo los obtuvo. Pero esto en modo alguno implica que el hecho de "revelar a otro" no se haya producido, ya que son dos acciones distintas e independientes (el obtener los datos y el revelarlos).

La conclusión del tribunal nos parece acertada. De alguna forma, es de esperar que la aplicación de estos nuevos delitos impondrá un límite a la libre circulación de toda clase de datos personales que a diario vemos en internet. Hoy día existe un verdadero "mercado negro" de informes personales, donde, sin permiso de sus titulares, se venden y compran ilegalmente cientos de datos.

2.- Acceso ilegítimo a un sistema informático

El tribunal luego analiza el segundo hecho. Recordemos que se investigaba el acceso a tres cuentas de correo electrónico de otros usuarios, su manipulación y alteración sin permiso del titular del sistema informático.

La sala, partiendo de los dichos del imputado (6), describe el hecho como "acceder y alterar la base de datos de clientes de correo electrónico ... para luego adueñarse de las cuentas que se mencionan y usarlas a su modo". El tribunal entiende que no hay delito: "...si bien resulta indiscutible que la conducta expuesta importó una invasión de la intimidad de las personas afectadas, no menos cierto es que tal intrusión no adolece de la condigna protección penal".

(3) Cabe aclarar que toda la doctrina nacional es conteste en este sentido.

(4) O un empleado, dentro de la empresa, debió facilitárselo.

(5) Aquí podría entrar en juego el párr. 1º del art. 157 bis CPen. si se logra probar que alguien a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accedió, de cualquier forma, a un banco de datos personales. A nuestro entender, esta norma incluye no sólo el acceso digital, sino también el acceso físico al lugar donde están los datos personales (el tipo dice "de cualquier forma").

(6) En su defensa alegó que su introducción en la configuración del sistema de correo electrónico de Fibertel fue el producto de su propia investigación de la falla de seguridad de la empresa, que él había detectado en su cuenta.

(7) Palazzi, Pablo, "El acceso ilegítimo a un sistema informático" (JA 1999-3-21).

(8) La ley define en su art. 2 al "archivo, registro, base o banco de datos" de la siguiente forma: "Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso". Para el alcance de esta norma según una perspectiva del derecho comparado y de los fundamentos de la ley 25326 (LA 2000-D-4363) ver Palazzi, Pablo, "La protección de los datos personales en la Argentina", 2004, Ed. Errepar, comentario al art. 2.

No estamos muy convencidos de esta afirmación. Si bien en nuestro derecho penal no está tipificado el acceso ilegítimo a un sistema informático (7), el art. 157 bis inc. 1 CPen. penaliza el acceso ilegítimo a una base de datos (que en teoría se encontrará dentro de un ordenador o sistema informático). Entonces, si bien no constituye delito el acceso ilegítimo a un ordenador, sí es delito el acceder a un banco de datos personales sin autorización legal. Partiendo de la propia descripción del hecho por parte del tribunal (que a su vez se basa en los dichos del imputado) se da, a nuestro entender, el hecho típico que la ley enuncia como "...accediere, de cualquier forma, a un banco de datos personales".

Veamos. La empresa afectada tiene los correos electrónicos en una base de datos o en un "conjunto organizado de datos personales", conforme a la definición dada por el art. 2 ley 25326 (8), que el tribunal omite mencionar. Tampoco estaba en discusión que el imputado accedió a los mismos. Y que en ellos había datos personales de terceros, esto es, las cuentas de correo electrónico. El correo electrónico es una forma de comunicación estática, no dinámica, pues no tiene lugar en tiempo real. Requiere además que el intermediario (el ISP.) y los extremos de la comunicación almacenen estos datos personales. En todo correo electrónico hay datos personales del emisor y del receptor. En el caso existía, asimismo, un sistema de seguridad de datos que fue el que el imputado burló para entrar en la base de datos personales. En esta conclusión no hay analogía de ninguna especie, sino simple interpretación de la ley.

Luego el tribunal se refiere al bien jurídico protegido y al efectivo perjuicio. Así, concluye que "... conforme a la prueba acumulada no se advierte que su actividad haya ocasionado perjuicio, ni tampoco que encuentre respuesta punitiva en alguna de las tipicidades previstas por el Código Penal, en tanto según se desprende del art. 1 ley 25326, la misma tiene por objeto 'la protección integral de datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes' y es justamente esta última aplicación la que no guarda relación con el acto que se reprocha".

El tribunal realiza por una parte una interpretación extensiva de la ley 25326 incorporando en el tipo penal del art. 157 bis CPen. al concepto de banco de datos el término "destinados a dar informes" (mencionado en el art. 1 y en otros de la ley como los arts. 14, 15, 29 inc. h, 33 y 35), y de allí concluye —entendemos— que la base de datos de un proveedor de acceso a internet (en el caso, de Fibertel) no entra dentro de tal supuesto.

Sin embargo, los tipos de la ley 25326 (tanto el art. 117 bis como el art. 157 bis CPen.) no exigen que el banco de datos esté destinado a proveer informes, ni siquiera que sea público o privado. Sólo se refieren a archivos o bancos de datos personales. Esta ausencia del término "destinado a proveer informes" la encontramos también en otros artículos de la ley (arts. 8, 19, y 40). Al usar en ambos incisos el término "banco de datos personales" el tipo penal del art. 157 bis CPen. incluye a registros tanto públicos como privados y a aquellos que son tanto de uso interno como externo, o que proveen información a terceros.

Tanto el art. 117 bis como el art. 157 bis CPen. no parecen exigir perjuicio alguno (salvo lo dispuesto en el inc. 3 del art. 117 CPen.). Por ende no debió hablarse de perjuicio, el cual, por otra parte, debe presuponerse cuando se accede a correspondencia digital ajena.

Esto ha sido claramente señalado por la doctrina, que al comentar esta nueva figura señaló: "Las intromisiones informáticas alcanzan así por primera vez protección penal a través de este nuevo instituto del hábeas data, consagrando así la protección de la privacidad de sus archivos respecto de terceros indiscriminados... (casos típicos de *hacking*), sin exigir ningún tipo de modificación de tales datos, ya sea por borrado, adulteración, o agregados, o copiado de información. Estamos así ante un delito de peligro abstracto que pone de relieve la alta protección que se le quiere brindar a los registros privados y públicos de datos con el fin de garantizar la intimidad y el honor de las personas físicas, y la protección de la información relativa a personas jurídicas (conf. art. 2 de la ley)" (9).

La citada autora luego agrega: "Podríamos preguntarnos si la violación de secretos prevista especialmente en la ley de hábeas data no resulta sobreabundante, ya que existe una norma de carácter general que castiga toda violación de secretos por noticias adquiridas en un oficio o empleo (art. 156 CPen.). Entendemos que su inserción en la ley resulta adecuada, ya que además de la función didáctica que significa su inclusión en esta nueva norma de la cual

emerge con gran significancia el deber de confidencialidad, es del caso destacar que la figura aquí descripta tiene menos exigencias típicas que el mencionado art. 156 CPen. En efecto, *no requiere que la divulgación del secreto pueda causar daño. La sola revelación a otro de este tipo de información, sería punible, porque la ley establece a priori que la esfera de reserva e intimidad de una persona, merece ser preservada.* De esta manera se consagra que los registros de datos incluidos en la ley, son secretos, y están protegidos sin necesidad de tener que demostrar que su quebrantamiento puede producir daños de alguna otra índole: patrimoniales, físicos, morales o afectivos, tal como lo exige la violación de secretos normada por el art. 156 CPen."

Por otra parte, la transcripción del objeto de la ley (art. 1) hecha por el tribunal es parcial. La norma en toda su extensión dice: "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43 párr. 3º CN.". Mediante esta ley, entonces, lo que se ampara es el secreto y la privacidad (en este caso, de datos personales), que, por otra parte, coincide con el bien jurídico tutelado también en la violación de secretos (10), que es el capítulo del Código Penal donde esta figura fue insertada por la ley 25326. La afectación a este bien jurídico tiene lugar cuando un tercero sin consentimiento del prestador del servicio (11) ni del titular de la cuenta de correo electrónico ingresa a ella.

La forma más clara de ver la interpretación a la que lleva la tesis del fallo es comparar el caso bajo análisis con uno similar en el mundo *offline*. Supongamos que una persona desea comprobar si el correo epistolar es seguro y para ello entra una noche subrepticamente en el edificio de una empresa de correos, abre unas cuantas sacas de correspondencia y se dedica a leer cartas privadas que los usuarios han enviado y que todavía no han sido distribuidas. Tal acción queda atrapada por el delito de violación de correspondencia, y probablemente también por el de violación de domicilio. Si dicho sujeto alegara que sólo quería demostrar las fallas de seguridad de la empresa (incluso para que ésta las mejorase), tal intención en modo alguno debería afectar la configuración del tipo penal.

(9) Lenardón, Ana M., "Régimen de penalidades contenidas en la ley 25326 de Protección de Datos Personales", rev. Derecho y Nuevas Tecnologías, ns. 4-5, p. 315.

(10) Soler, al referirse a estos delitos, habla de una "esfera protegida de intimidad" (Soler, Sebastián, "Derecho Penal argentino", t. IV, 1992, Ed. TEA, p. 114).

(11) Por ejemplo, no hay ilegalidad cuando un empleado del ISP., a pedido del titular, debe investigar un problema con el correo electrónico y accede a un mensaje. O cuando, en virtud del art. 10 párr. 2º ley 25326, existe justa causa para la revelación del secreto. Ver Lenardón, Ana M., "Régimen de penalidades contenidas en la ley 25326 de Protección de Datos Personales" cit., p. 316.

Pero en este caso parece que el mundo *on line*, que justamente es el que más necesita protección porque es donde resulta más fácil violentar la privacidad de cualquier individuo, dada la existencia de estándares abiertos, es también el más desprotegido legalmente, pese a la expresa intención del legislador de amparar el ingreso sin permiso a una base de datos.

b) La protección penal del derecho del compilador

La compilaciones y bases de datos fueron tradicionalmente amparadas por el derecho de autor. Pero a diferencia de otras clases de obras donde se exigía originalidad a la obra misma, la originalidad de la compilación no reside en la obra sino en la disposición y selección de sus elementos (12). Si adicionalmente esta obra está compuesta de otras obras intelectuales, cada una de estas obras individuales incorporadas a la colección —con el debido permiso de sus respectivos autores— podrá tener su protección independiente como tal.

1.— El caso “Nosis v. Axesor”

En el caso “Axesor” se consideró que existió copia de una base de datos. Se calificó tal conducta como infracción a la Ley de Propiedad Intelectual. El imputado había accedido a través de un sitio de consulta de internet al servicio “Sistema Alerta Crédito” (SAC.), brindado onerosamente por la firma Nosis para copiar los datos exclusivos de la base de datos para su comercialización como información financiera en su página de internet. La Cámara de Apelaciones (13), en una decisión de fecha 31/3/2005, confirmó el fallo del juez de primera instancia que había considerado delito la conducta analizada.

Al analizar la prueba el fallo señala las conclusiones de los peritos sobre la diferencia de la información existente en ambas bases de datos. Si bien la información que componía la base de datos se suele obtener de fuentes de acceso público, el compilador puede alterar ciertos datos para descubrir luego quién los copia. Aparentemente la

demandada copiaba la información pero la cambió para evitar que se detectara esta copia. Sin embargo, ciertos patrones en común quedaron, como ser algunos errores voluntarios de carga de datos (14), o las fechas, que al ser cambiadas masivamente por la querellada derivaron en que la base de datos plagada contuviera fechas que caían en días feriados —lo cual es imposible en una operación bancaria—, o la existencia de datos que el Banco Cenal de la República Argentina sólo hizo disponibles a partir de cierta fecha, posterior a la constitución de la demandada (15). Otros códigos coincidían numéricamente con los de la querellante, pero se probó que la empresa querellada había agregado un “200” delante para “diferenciarlos”. De este modo, según explica el fallo, quedó probado que la demandada *no había obtenido en forma independiente la información sino que la había copiado de las bases de datos de la querellante*.

En este caso concreto había mucha información que era exclusivamente producida por la empresa querellante. Más allá de que muchas de las fuentes suelen ser públicas en esta industria (y, por ende, los datos que las componen son de dominio público), aun cambiando automáticamente ciertos datos, había registros, formas y objetos que en su totalidad funcionaban como “trampas”, o que no eran datos reales, y que sólo sirven para probar la copia de parte de la obra (16).

Quedó probado que había una copia; sin embargo, creo que la cuestión en este caso era determinar si había o no una “obra protegible” por el derecho de autor.

Las impresiones del fallo han sido dispares. Ciertos autores, poniendo énfasis en la “injusticia” de quien se aprovecha del trabajo ajeno, sostuvieron que la decisión era acertada. Así, Horacio Granero, al comentar este mismo fallo, sostiene que no sancionar al obrar de quienes copian ilegítimamente y sólo con una finalidad comercial bases de datos ajenas importa *premiar al que de manera desleal y parasitaria se aprovecha de la inversión y el esfuerzo ajenos* (17). A nuestro modo de ver el problema, la opinión

(12) Ver Palazzi, Pablo, “Alternativas legales para la protección de bancos de datos” (JA 2004-1-1204), leyes y autores allí citados, y Goldstein, Mabel, “Derecho de autor y sociedad de la información”, 2005, Ed. La Rocca, p. 322; Dessemontet, François, “Le droit d’auteur”, 1999, CEDIDAC., Lausanne, p. 729 y ss. (con relación al derecho suizo); criterio legal que también encontramos en el CPI. francés, cuyo art. L.112-3 dispone (ley 96-1106 del 18/12/1996): “Les auteurs de traductions, d’adaptations, transformations ou arrangements des oeuvres de l’esprit jouissent de la protection instituée par le présent Code sans préjudice des droits de l’auteur de l’oeuvre originale. Il en est de même des auteurs d’anthologies ou recueils d’oeuvres diverses qui, par le choix et la disposition des matières, constituent des créations intellectuelles”; y en Estados Unidos, conforme a la definición del término “compilation”, en la Copyright Act de 1976.

(13) C. Nac. Crim. y Corr., sala 1ª, del 31/3/2005, “Shakery Rodríguez, Carlos B.”.

(14) A veces ciertos errores inocuos son introducidos adrede por el productor del banco de datos para generar una prueba de la eventual copia, como ocurrió en el caso “Errepar v. Nahas” (JA 2003-3-480). En similar postura, aceptando que la existencia de errores constituye clara prueba de la copia de partes de la obra intelectual, ver los casos norteamericanos: “Financial Information, Inc. v. Moody’s Investors Service, Inc.”, 599 F. Supp. 994, p. 996. n. 3 (SDNY., 1983), y “Central Telephone Co. of Virginia v. Johnson Publishing Co.”, 526 F. Supp. 838 (D.Colo., 1981), p. 844.

(15) Se señala, por ejemplo, la comunicación A-3245 (30/3/2001), publicada en el B.O. del 11/4/2001 (LA 2001-B-2235).

(16) Tal como ocurrió en el caso “Errepar” ya citado.

(17) Conf. Horacio Granero, “La protección legal de las bases de datos (un fallo ejemplar)”, en El Dial del 4/5/2005 (www.eldial.com.ar).

de Granero tendría fundamento en el derecho de la competencia desleal, pero no en el derecho de autor.

Lamentablemente, la figura penal que tutela en nuestro derecho la sana concurrencia entre competidores reprimiendo la concurrencia desleal ha resultado en la práctica ineficaz (soy generoso con el adjetivo) y, por ende, de escasa aplicación en nuestro medio. Esto lo demuestran la jurisprudencia y las críticas doctrinarias a la figura del art. 159 CPen. y a las normas genéricas del Derecho Privado (18). Se ha dicho que la competencia es la lucha por la clientela y que el premio es la propia clientela (19), pero si no se cuenta con una adecuada protección y sanción contra quien se sale de las reglas no sólo no se obtiene el premio, sino que incluso existe un incentivo para no cumplir esas reglas. Está claro que nos hace falta en la Argentina una ley que reprima civil y penalmente la competencia desleal (20), amparando uno de los bienes más preciados y difíciles de conquistar para las empresas: la clientela.

Para la tesis de Granero, entonces, basta con probar un simple esfuerzo de recopilación ante un tribunal para hacerse merecedor de una protección sobre esos datos (aunque la selección no sea original pero demuestre esfuerzo en esa recopilación). De alguna forma se reemplaza la originalidad propia del derecho de autor por el esfuerzo, lo que ha dado en ser llamado doctrina delo "sudor de la frente" ("*sweat of the brow*").

Por otra parte, justamente al comentar este mismo caso, Frene sostiene (21) que la decisión no es acertada. Considera que las compilaciones están sólo amparadas por la selección y disposición de sus contenidos y que, por ende, los elementos que las informan no estarían amparados por el derecho de autor.

El autor funda esta tesis –que podríamos llamar "débil" o "acotada" de protección de bases de datos– en el art. 10 del Acuerdo TRIPs., que establece la protección para las compilaciones de datos por razón de su selección y dis-

posición de sus contenidos, y siempre que sean creaciones. Los datos *per se* no reciben protección, y pueden ser copiados por cualquiera sin infringir las leyes de derecho de autor. Funda sus conclusiones también en el art. 17 CN., que dispone que todo autor o inventor es propietario exclusivo de su obra, invento o descubrimiento por el término que le acuerde la ley. Razona que las compilaciones de datos normalmente tienen un "autor", que es quien elige qué datos incluir, en qué orden, cómo presentarlos, etc., y es por ello que pueden recibir la protección de la ley 11723. Los datos, por el contrario, no tienen autor, no deben su existencia a nadie en particular, incluso la persona que descubre un dato no es su "autora". Se trata de información sobre la cual nadie puede atribuirse la autoría ni la propiedad. El citado autor termina ejemplificando lo ocurrido en Estados Unidos con el caso "Feist" y propone la necesidad de una legislación específica en la materia (al estilo del *derecho sui generis* europeo). En el caso "Feist" la Corte Suprema de Estados Unidos sostuvo en el año 1991 que un directorio telefónico no estaba amparado por el derecho de autor, ya que la compilación era banal y carecía de la selección y disposición necesarias para su protección legal.

La posibilidad de amparar las bases de datos no originales, esto es, las que se encuentran integradas por datos, hechos o elementos no protegibles –como la del caso que comentamos–, es un tema muy discutido en el Derecho de Autor comparado.

En los Estados Unidos primó durante tantos años la doctrina del "sudor de la frente" apoyada en la *Copyright Act*, hasta que fue desbancada en el caso "Feist". En la Unión Europea las diferencias que existían también entre los diversos países (22) antes de la directiva que creo un *derecho sui generis* sobre bases de datos (23) demuestran que el derecho de autor puede amparar estas creaciones más allá de su originalidad. Nótese, por ejemplo, que en el caso "Feist" los tribunales de primera y de segunda instancia

(18) Usieto-Blanco, Alberto, "La defensa de la competencia en la experiencia argentina", en "El nuevo régimen del Derecho de la Competencia", 2001, Universidad de Montevideo, Montevideo, p. 90 (criticando las normas penales y su interpretación jurisprudencial); Cabanellas, Guillermo (h) y Bertone, Luis, "Derecho de Marcas", t. II, 2003, p. 573 (referencia a la ineficacia del art. 159 CPen.); Míguez, Isabel, "La empresa y las responsabilidades emergentes de la competencia desleal", *rev. Prudentia Iuris*, agosto de 2000, n. 52, p. 33 (señalando el escaso desarrollo del derecho de la concurrencia en la Argentina); Cabanellas, Guillermo (h), "Derecho de las patentes de invención", t. 1, 2004, Ed. Heliasta, p. 182 (señala la necesidad de implementar legislativamente el art. 10 bis del Convenio); García Menéndez, Sebastián, "Competencia desleal", 2005, Ed. LexisNexis, p. 41; Spolansky, "El delito de competencia desleal y el mercado competitivo" (quien parece ser el autor más optimista en la materia, pese a ser el único penalista de esta lista de autores que he citado).

(19) Garrigues, "Temas de Derecho vivo", p. 199.

(20) Proyectos no han faltado; ver Chaloupka, Pedro, "La competencia desleal en la Argentina. Informe y propuesta legislativa", en "Derechos intelectuales", vol. 5, Ed. Astrea, p. 139.

(21) Frene, Lisandro, "La protección de las bases de datos bajo la ley 11723", ED del 13/6/2005.

(22) Powell, Mark, "The EC draft Database Directive: a revolutionary means of protecting databases", en *The International Computer Lawyer*, vol. 2, n. 3, marzo de 1994, p. 11.

(23) Sobre el *derecho sui generis* ver Bouza López, Miguel, "El *derecho sui generis* del fabricante de bases de datos", 2001, Ed. Reus.

habían citado abundante jurisprudencia (24) que sostenía que los directorios telefónicos eran amparables por el derecho de autor. Pero de un día para el otro la Corte Suprema de Estados Unidos revocó ese fallo de la Cámara de Apelaciones (25) que, al confirmar el de primera instancia (26), había dado amparo a esta base de datos no originales (un listado de teléfonos de una zona de Kansas).

Se trataría aparentemente de una cuestión del enfoque y fundamentos que se le quiere dar al derecho de autor. Creo que los vaivenes de la jurisprudencia comparada son demostrativos de ello, incluso en el derecho continental, que es la base de nuestro derecho de autor.

La influencia del caso "Feist" en la desprotección de compilaciones "no originales" ha sido muy fuerte. En internet, por ejemplo, donde existen grandes colecciones de información conformadas por elementos no originales, los casos más recientes demuestran que es muy difícil recurrir a la *Copyright Act* para amparar esta clase de obras (27). Por eso se recurre a alternativas como son las normas sobre protecciones tecnológicas, los contratos, el delito de acceso ilegítimo (ver el caso que comentamos en el próximo punto), los nuevos derechos, como el derecho *sui generis*, y hasta el incremento significativo del plazo de protección de obras intelectuales (28).

Si bien compartimos la tesis que sostiene que la extracción de datos no originales –vgr., fallos, normas (29), noticias, datos climáticos, resultados de deportes, hechos en general– de una compilación no está amparada por el derecho de autor (30) (si no más bien por la protección contra competencia desleal), en el presente caso de la prueba surge que existió una extracción sistemática y parasitaria de las bases de datos de la querrela, que equivale a la copia total de la obra intelectual (incluyendo la selección y disposición dada por el compilador).

2.– El caso "Reidman"

En el caso "Reidman" (31) se consideró que constituía administración fraudulenta el acceso a un banco de datos de informes crediticios utilizando claves que pertenecían a una entidad bancaria donde antes trabajaba el imputado.

En el caso el ex empleado de una sucursal bancaria, luego de cesada la vinculación laboral, utilizó en numerosas oportunidades la clave de acceso –que conocía a raíz de su anterior trabajo– para acceder a una base de datos que vendía informes crediticios. Esto le permitió acceder a esa información, que se facturó al banco (suscriptor del servicio) y no a la cuenta que éste poseía en el locutorio con la empresa Organización Veraz.

En primera instancia se procesa al imputado como autor del delito de acceso ilegítimo a banco de datos personales, en concurso ideal con estafas reiteradas –diecisiete hechos–, todas ellas en concurso real entre sí (arts. 157 *bis inc. 1* y 172 CPen.). La Cámara, en el caso que comentamos, confirmó el procesamiento pero cambió la calificación legal de los hechos.

El primer aspecto que destaca la Cámara es uno probatorio: encontró suficientes los diversos peritajes llevados a cabo por la División Inteligencia Informática de la Policía Federal Argentina para establecer que desde las computadoras ubicadas en el locutorio se requirieron por internet a la Organización Veraz al menos diecisiete informes en los que se utilizaron un usuario y una clave distintos de los autorizados (los correspondientes al Banco de Boston, sucursal Unicenter), por lo cual el costo de dichas consultas fue asignado a la referida entidad bancaria en lugar de facturarse a la cuenta que poseía el locutorio con la firma Veraz. A esto se suman los dichos del propio imputado (quien declaró estar a cargo del locutorio y haber trabajado en el banco) y de sus familiares y la acusación de un

(24) Ver "Hutchinson Telephone Co. v. Fronteer Directory Co.", 770 F.2d 128 (8th Cir., 1985); "Southern Bell Telephone & Telegraph Co. v. Associated Telephone Directory Publishers", 756 F.2d 801 (11th Cir., 1985); "Leon v. Pacific Telephone & Telegraph Co.", 91 F.2d 484 (9th Cir., 1937); "Central Telephone Co. of Virginia v. Johnson Publishing Co.", 526 F. Supp. 838 (D.Colo., 1981); "Southwestern Bell Telephone Co. v. Nationwide Independent Directory Service, Inc.", 371 F. Supp. 900 (W.D.Ark. 1974); "Southern Bell Telephone & Telegraph Co. v. Donnelly", 35 F. Supp. 425 (S.D.Fla. 1940); "Cincinnati and Suburban Bell Telephone Co. v. Brown", 44 F.2d 631 (S.D.Ohio 1930); "Hartford Printing Co. v. Hartford Directory & Publishing Co.", 146 F. 332 (D.Conn. 1906).

(25) 916 F.2d 718.

(26) 663 F. Supp. 214.

(27) Ver, por ejemplo, Huse, Charles C., "Database protection in theory and practice: three recent cases", en 20 Berkeley Tech. L.J. 23 (2005).

(28) La expansión de plazos tuvo su punto culminante en México, con 100 años de protección para obras intelectuales. Estos plazos tan extensos han sido objetos de mucha crítica. Ver Ginsburg, Jane C., "How copyright got a bad name for itself", 26 Colum J L & Arts 61, 65 (2002) (donde se critica esta extensión indefinida de los plazos).

(29) Ver caso "Errepar" cit. (JA 2003-3-480).

(30) Pues, como vimos, estos datos, *per se*, carecen de originalidad y de autor.

(31) C. Nac. Crim. y Corr., sala 7ª, del 18/3/2005, causa 24848, "Reidman, Alejandro".

empleado del Departamento de Seguridad de la citada entidad financiera.

El segundo aspecto del fallo de Cámara es la calificación legal asignada a los hechos. El tribunal, a manera de advertencia, aclara que no ingresará a la polémica que divide a la doctrina en torno a la tipicidad de la conducta de valerse de un proceso informático para obtener en forma gratuita un servicio arancelado, en este caso, información.

El tribunal concluye que el imputado "defraudó los intereses que le confiara el Banco de Boston al utilizar información confidencial (*nombre de usuario y clave de acceso de la base de datos de la Organización Veraz*), en su provecho y en detrimento de la empresa a la que estaba unido en aquel entonces por un contrato laboral, que le sirvió de 'llave' para desviar en aquélla el débito que sus consultas insumían, configurando dicho accionar el tipo del art. 173 inc. 7 CPen."

La calificación del delito como administración fraudulenta podría ser discutible, pues la relación de empleo ya había cesado. El imputado no administraba nada, sino que conocía esas claves porque las usaba en su trabajo. Es cierto, sin embargo, que debía abstenerse de usarlas en su provecho y en perjuicio de su ex empleadora. Más bien parece que existió una especie de abuso de información privilegiada (32). Si bien la información no puede ser objeto de los delitos de hurto o robo, sí es posible que el acceso, uso o apropiación de ciertos conocimientos constituya violación de secretos comerciales. El secreto comercial incluye todo lo relativo a la organización interna y a las relaciones de la empresa (33). En la Argentina la ley 24766 (LA 1996-C-3378) ampara esta clase de información confidencial, conocida como "secretos comerciales". Sin embargo, para ser tales deben referirse a información cuya revelación afecte la capacidad competitiva de la empresa. Por eso el art. 1 inc. b de la citada ley exige como recaudo que dicha información "tenga un valor comercial por ser secreta". Éste no era el caso respecto de la entidad financiera.

En cuanto al acceso a la base de datos señaló lo siguiente: "Por otra parte, el tribunal entiende que ... se da un caso de consunción entre la administración fraudulenta y el acceso ilegítimo al banco de datos personales" (art. 157 bis inc. 1 CPen.), porque "uno de los tipos comporta una valoración tan francamente superior, que tanto el tipo como la pena de la figura más grave realizan cumplidamente la función punitiva no ... sólo por cuenta propia, sino por cuenta del otro tipo" (34).

También hay que tener en cuenta que ambos delitos protegen no sólo bienes jurídicos distintos sino también a personas diferentes. La administración fraudulenta, como delito contra el patrimonio, sin lugar a dudas amparó al banco, que se vio obligado a pagar consumos de información que no realizó. El acceso ilegítimo ampara a la empresa de informes comerciales, que es la propietaria del banco de datos. El delito del art. 157 ampara la confidencialidad de esa información, pues, tal como lo evidencia el título en el cual está inserta la norma, se trata de una violación de secretos.

La lectura del caso "Reidman" nos da la impresión de que de alguna forma se termina protegiendo al banco de datos en su valor comercial en forma indirecta, no porque el mismo sea una compilación de datos que como obra intelectual tenga mérito en la selección y valoración de sus elementos, sino porque se ingresó al mismo sin permiso. De alguna forma el acceso ilegítimo a una base de datos —considerado como delito en este caso— permite a la empresa afectada proteger la clientela, puesto que el uso gratuito de la misma es una forma de competir deslealmente sin pagar el acceso correspondiente.

Tanto "Reidman" como "Axesor" son fallos que demuestran que en nuestro país existe una amplia protección para el compilador de bases de datos, ya sea porque la selección y disposición de los elementos que los componen en su conjunto constituyen una obra intelectual amparada por la ley 11723 (ALJA 1853-1958-268) como porque el acceso a las mismas sin permiso del titular (con claves ajenas) puede constituir un acceso ilegítimo en los términos del art. 157 bis CPen.

(32) Conf. Bacigalupo, Enrique, "Derecho Penal Económico", 2000, Ed. Hammurabi, p. 431.

(33) Gómez Segade, José, "El secreto industrial", 1974, Madnd, ps. 51 y 52.

(34) Soler, Sebastián, "Derecho Penal argentino", t. II, 1978, Ed. TEA, Río de Janeiro, p. 175.