Departamento de Derecho

Maestría en Derecho Penal

Skimming y *phishing* de tarjetas de crédito o débito: ¿actos preparatorios o principio de ejecución de la defraudación cometida mediante tarjeta falsificada o el uso de sus datos?

Alumno: Francisco Divito (DNI 37.541.679)

Tutor: Magíster Guillermo Orce

Ciudad Autónoma de Buenos Aires, 12 de abril de 2021

Índice temático

Resumen:

En el presente trabajo se analiza si las maniobras de obtención ilegítima de información de tarjetas bancarias, identificadas como *skimming* y *phishing*, constituyen actos preparatorios o importan el comienzo de ejecución de las defraudaciones cometidas mediante tarjetas de crédito o débito falsificadas y/o el uso no autorizado de sus datos.

Al efecto, se comienza con un abordaje teórico de dichas modalidades de captación de datos, así como de los posibles tipos penales en juego: tenencia de instrumentos destinados a falsificar, falsificación de tarjetas, fraude con tarjetas, entre otros. Luego se estudia la incidencia que el *skimming* y el *phishing* tienen en el *iter criminis* de las defraudaciones en cuestión a la luz de las distintas teorías vinculadas a la delimitación entre actos preparatorios y ejecutivos de delitos y del desarrollo jurisprudencial sobre la materia. A partir de ello, se analiza la posibilidad de crear un tipo penal de adelantamiento que incluya dichas conductas.

I. Primeras aproximaciones al objeto de estudio

Decir que la llamada sociedad de la información debe su expresión a los avances y el uso intensivo de las tecnologías de la información y comunicación no es novedoso. En la actualidad, en gran parte debido a la evolución de las redes telemáticas, las personas acceden, transmiten y manipulan información a diario y cada vez con mayor facilidad. Pero es sabido que los innumerables beneficios de estos avances traen aparejados nuevos riesgos y que, en algunos casos, estos se traducen en materia de interés para el Derecho Penal. En este sentido, se ha advertido que "surgen modalidades delictivas dolosas de nuevo cuño que se proyectan sobre los espacios abiertos por la tecnología"[1], entre estas, "[l]a criminalidad asociada a los medios informáticos y a *internet*"[2]. En función de ello es que corresponde analizar, ante la velocidad con la que crecen las tecnologías y los delitos vinculados a estas, si nuestro ordenamiento jurídico responde a tal dinamismo y, en caso afirmativo, si lo hace de manera adecuada.

En el marco de la Parte Especial del Derecho Penal, uno de los ámbitos en los que este fenómeno se manifiesta con claridad es, dentro de los delitos contra la propiedad, el correspondiente al delito de estafa y las formas modernas de defraudación en cuya comisión se utiliza la tecnología. Resulta que junto con los avances tecnológicos fueron apareciendo distintos modos de lesionar patrimonios ajenos que obligaron a la doctrina a reflexionar sobre la estructura típica de la estafa, conformada por los elementos engaño, error, disposición patrimonial y perjuicio. Incluso el legislador se vio obligado a introducir modificaciones al Código Penal que respondieran a dichos cambios (v.gr., leyes 25.930 y 26.388). Así, antes de la sanción de estas leyes se discutía, por ejemplo, si las maniobras que producen perjuicios patrimoniales mediante la utilización de aparatos mecánicos -cajeros automáticos, entre otros- podían ser subsumidas en el tipo de estafa cuando, en rigor, "como este delito requiere un engaño que produzca un *error* en *otro*, lo cierto es que ni estos aparatos son *otro* ni concurre la exigencia de que el sujeto pasivo haya sufrido un *error*, entendido como una falsa representación de la realidad"[3]. Este y otros debates, como se verá, perdieron virtualidad tras la entrada en vigencia de las leyes mencionadas.

[1] SILVA SÁNCHEZ, *La expansión del Derecho Penal*, 3.ª ed., BdeF, Montevideo-Buenos Aires, 2011 [1999], p. 14.
[2] SILVA SÁNCHEZ, *La expansión del Derecho Penal*, 2011 [1999], pp. 14 y 15.
[3] RIGHI, *Delito de estafa*, 2.ª ed., Hammurabi, Buenos Aires, 2017 [2015], pp. 269 y 270; BACIGALUPO, *Estudios sobre la parte especial del derecho penal*, Akal, Madrid, 1991, p. 176.

En este contexto es que surge la necesidad de reflexionar sobre algunos aspectos de estas formas modernas de defraudación como, en lo que aquí interesa, la incidencia que las maniobras de captación de datos de tarjetas de crédito y débito u otros -v.gr., *skimming* y *phishing*- tienen en la posterior defraudación cometida mediante tarjetas falsificadas o el uso no autorizado de sus datos. ¿Configuran dichos comportamientos el comienzo de la ejecución de estos delitos o son solo parte de su preparación? Y, acaso fuera esta última la respuesta correcta, ¿deberían crearse nuevas figuras penales que prohíban esas conductas?

A partir de este disparador es que abordaré estas modalidades delictivas con la intención de analizar -desde una mirada integral que abarque también institutos de la Parte General- su correspondencia con nuestra legislación vigente. A tal fin, se presentará en primer lugar el marco teórico de estas técnicas de captación ilegítima de información y de los tipos penales en juego. Luego, se analizará si estas configuran el comienzo de la ejecución de alguna defraudación especial o si, por el contrario, solo forman parte de su preparación. Finalmente, de determinarse que esta última es la opción correcta, se estudiará si resulta o no conveniente regular dichas conductas de manera autónoma, adelantando la penalidad.

Antes de comenzar, permítaseme una aclaración. La temática de las formas modernas de defraudación y, más aún, de la criminalidad asociada a la tecnología como un todo, es una materia en constante desarrollo que abarca un sinfín de tecnicismos y problemáticas de difícil abordaje en un trabajo con las limitaciones de extensión que tiene el presente. Ello no será, bajo ningún concepto, motivo para esquivar la profundidad que el estudio de la disciplina merece, pero sí razón para abordar el análisis de las modalidades de captación de datos mencionadas y su vinculación con el principio de ejecución de la de defraudación desde una mirada estrictamente jurídica y no técnico-informática -para lo cual, por cierto, existe la bibliografía especializada en cuestiones informáticas a la que haré referencia-.

II. *Skimming* y *phishing* como modalidades de obtención no autorizada de datos

A. Marco teórico

Uno de los cambios que significó un gran beneficio a la sociedad ha sido la sustitución del pago con dinero por otros medios (por ejemplo, tarjetas de crédito y débito). Pero ya en 2004 se advertía que "[l]a utilización de estos medios de pago, a la par de sus ventajas, trae aparejada la posibilidad de que se vea afectada la propiedad de

modos distintos de los conocidos hasta hace algunas décadas atrás"[4]. Así, junto con esta evolución en las formas de pago apareció, por ejemplo, la modalidad delictiva comúnmente llamada *skimming*.

El término *skimming* es utilizado para identificar el acto de copiar los datos contenidos en la banda magnética de una tarjeta de crédito y/o débito. Usualmente se lo asocia con la colocación en cajeros automáticos de dispositivos que leen y registran los datos de las tarjetas que allí se introducen, aunque también se presenta en comercios en los que, por ejemplo, la persona encargada del cobro aprovecha el momento en el que tiene en su poder la tarjeta de pago para hacerse de sus datos mediante la utilización de este tipo de aparatos -comúnmente llamados *skimmers*-. En general, dicha información es luego reproducida en una tarjeta falsa con la que se realizan compras que son imputadas a la cuenta del titular de la tarjeta original o se extrae dinero de cajeros automáticos, entre otras modalidades; pero también puede ocurrir que se obtengan esos datos con la única intención de venderlos. En el caso de las tarjetas de débito, la clonación suele estar acompañada de maniobras tendientes a obtener su clave, como la instalación de pequeñas cámaras o *sobreteclados* en cajeros automáticos[5].

En este sentido y a modo de ejemplo, en la práctica se presentan casos de *cloning* o *skimming* bancario como el resuelto por la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, que intervino en un hecho "consistente en la utilización de un dispositivo que permitiría capturar datos de las bandas magnéticas de las tarjetas a través de una lectora colocada disimuladamente sobre la boquilla genuina de un cajero electrónico, almacenando así la información que habilitaría su ulterior falsificación o duplicación para consulta, tratamiento no autorizado y desviación intencional de información o fondos de cuentas de los legítimos usuarios del sistema electrónico, habiéndose empleado en el caso en forma concomitante una cámara digital oculta en un dispositivo plástico del tipo folletero mediante la cual se filmaba a los circunstanciales usuarios del cajero intervenido con el objeto de registrar y obtener los códigos de acceso (PIN) a sus cuentas"[6].

---

[4] GOTTHEIL/LÓPEZ, "Nuevos delitos vinculados con tarjetas (A propósito de las modificaciones al Código Penal introducidas por la ley 25930)", en *Revista de Derecho Penal y Procesal Penal*, vol. 4, Lexis Nexis, 2004, p. 727.

[5] Ver GOTTHEIL/LÓPEZ, *Revista de Derecho Penal y Procesal Penal*, 2004, pp. 731 y 732.

[6] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.663, "OLIVEIRA RIVAS, Fabio y otros s/ defraudación", 20 de agosto de 2008 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020). En este fallo, sobre el que volveré más adelante, se analizó el grado de realización del tipo del art. 173, inc. 15, del Código Penal.

En definitiva, más allá de la modalidad a la que se recurra y de la finalidad que se persiga, lo cierto es que, a los fines del presente análisis, podemos incluir en el *skimming* las conductas por medio de las que se copia el contenido electrónico de una tarjeta bancaria con el uso de dispositivos útiles a tal efecto.

Otra de las modalidades delictivas que debe indiscutiblemente su existencia y evolución a los avances de la tecnología es el *phishing*. El término "viene de la palabra en inglés *fishing* (pesca), haciendo alusión al acto de 'pescar' usuarios mediante señuelos cada vez más sofisticados y de este modo obtener información financiera y contraseñas"[7]. Se lo acuña "para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas *web*, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. Además de datos económicos y financieros también se utiliza para captar todo tipo de datos personales y de contacto"[8]. La modalidad más frecuente -conocida como *deceptive phishing*-, que es la que aquí trataré, consta del envío masivo de correos electrónicos -que aparentan provenir de una institución de confianza como bancos y/o comercios- a distintos destinatarios para que estos informen sus datos por la misma vía o, incluso, para redirigirlos a sitios *web* clonados en los que cargan su información en la creencia de que operan realmente con dicha persona o entidad.

Para mayor ilustración y a modo de ejemplo, se puede mencionar el fallo resuelto por la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, en el que se analizaron "maniobras fraudulentas cometidas mediante 'phishing' que, en el caso, consiste en simular el envío de correos electrónicos de una entidad bancaria a sus clientes. Así, los destinatarios, son desviados a una 'página *web*' en la que ingresan los datos requeridos para acceder a sus cuentas. Posteriormente, la información es utilizada en forma ilegítima con el objeto de acceder a los fondos y efectuar transferencias a cuentas de terceros produciendo de tal modo el detrimento patrimonial"[9].

---

[7] TOSELLI/NICOLOSI LÓPEZ/CHOUELA, "Nuevas formas de defraudación: *phishing*", en *Revista de Derecho Penal y Procesal Penal*, vol. 2, Lexis Nexis, 2007, p. 309.

[8] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, Hammurabi, Buenos Aires, 2019, p. 119. En este sentido, véase también VANINETTI/VANINETTI, "Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet", en *El Derecho - Diario*, tomo 229, 2008, pp. 776 y ss. (cita digital ED-DCCLXX-349, 15 de septiembre de 2008).

[9] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.255, "BENTANCOUR, Yesica D. y otros s/ procesamiento", 13 de noviembre de 2018, (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020). En este fallo,

En todos los casos el resultado es el mismo: la información no es recibida por el banco, comercio o entidad de que se trate, sino por el pescador que luego los utiliza "para llevar a cabo fraudes económico-financieros o bien otro tipo de delitos contra la privacidad o la libertad de la víctima, entre muchos otros que pueden realizarse recurriendo a esta técnica de captación no autorizada de datos"[10]. Al igual que el *skimming*, el *phishing* es también utilizado con la intención de vender en la *Dark Web* (mercado negro digital) la información captada ilícitamente[11].

En definitiva, *skimming* y *phishing* son, aunque con sus diferentes características, maniobras de captación no autorizada de datos. Al respecto, no escapa a mi conocimiento que no son las únicas técnicas existentes con esa finalidad[12] pero, entiendo, sí las necesarias para abordar este análisis que pretende enfocarse en la incidencia que esta clase de conductas tienen en el *iter criminis* de posteriores defraudaciones. A todo evento, el desarrollo y las conclusiones del presente estudio podrían ser de utilidad a la hora de examinar comportamientos análogos.

Ahora bien, presentado brevemente este marco teórico descriptivo corresponde detenerse en la calificación legal que cabe asignar a las acciones mencionadas. Es que, como se verá más adelante, la determinación del tipo penal en el que una conducta debe ser encuadrada es una cuestión a tener en cuenta a la hora de delimitar el comienzo de la tentativa. Al respecto, dado que el *skimming* y el *phishing* no fueron tipificados de manera autónoma sino única e indirectamente mediante ciertas defraudaciones del artículo 173 del Código Penal, se partirá inicialmente de supuestos en los que se concreta un daño patrimonial tras realizarse la captación de datos, para luego determinar si las conductas en cuestión configuran el comienzo de ejecución de esos delitos. A tal fin, habrán de

sobre el que volveré más adelante, el hecho fue encuadrado en la defraudación prevista en el art. 173, inc. 16, del Código Penal.

[10] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "A diez años de la ley de delitos informáticos. Balances y propuestas", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 1, Hammurabi, Buenos Aires, 2019, p. 146.

[11] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, 2019, p. 119. Tal como los autores indican (ver nota al pie n.° 5 de la obra citada), según *I Profesional*, la venta de datos de una tarjeta de crédito activa ronda los 45 dólares en el mercado negro digital.

[12] A modo de ejemplo, se pueden mencionar brevemente otras: *smishing*, cuando en la captación se utilizan mensajes de texto de teléfonos móviles; *pharming*, cuando se explota una vulnerabilidad, por ejemplo, en los equipos de los usuarios para lograr redireccionar un nombre de dominio a una máquina distinta; instalación de un *keylogger* que permite registrar la actividad de una persona, por ejemplo, en su equipo de computación; entre otros. Ver al respecto VANINETTI/VANINETTI, *El Derecho - Diario*, 2008, pp. 776 y ss. (cita digital ED-DCCLXX-349, 15 de septiembre de 2008).

tenerse en cuenta, entre otras, las leyes 25.930 y 26.388 a partir de las cuales el legislador procuró abordar la temática en cuestión.

B. Calificación legal

Muchas de las controversias que pudieron haber existido en torno a la subsunción de las conductas fraudulentas vinculadas al uso de tarjetas bancarias perdieron cierta virtualidad tras la sanción de la Ley 25.930 en el año 2004. Es que esta, en su primer artículo, estableció la incorporación al Código Penal -como inciso 15 del artículo 173- del supuesto de defraudación especial de quien la cometiere "mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática"[13]. A su vez, en su segundo artículo, sustituyó la redacción del artículo 285 del código de fondo por una que equipara, a los efectos de los delitos de falsificación, las tarjetas de compra, crédito y débito a la moneda nacional. De este modo, por ejemplo, ya no tienen sentido las objeciones existentes para subsumir en este tipo penal el hecho de utilizar una tarjeta de origen ilícito para obtener dinero de un cajero automático, pues la norma mencionada prevé expresamente esa conducta como defraudación[14].

Liminarmente y en relación con esta última afirmación, creo necesario advertir dos cuestiones. En primer lugar, considero que, frente al modo en que ha sido redactada la fórmula típica vigente, cuando el perjuicio patrimonial es producido mediante el uso de una tarjeta bancaria -con las características requeridas por el texto legal- o de sus datos, la maniobra debe encuadrarse, en principio, como el supuesto especial de estafa allí legislado y no como un hurto del artículo 162 del Código Penal. Aunque es claro que lo distintivo de la estafa genérica del artículo 172 del código de fondo es que la víctima

[13] Art. 173, inc. 15, del Código Penal, incorporado por la Ley 25.930 (Boletín Oficial del 21 de septiembre de 2004).

[14] De esta opinión, RIGHI, *Delito de estafa*, 2017 [2015], p. 278; D'ALESSIO (Dir.)/DIVITO (Coord.), *Código Penal de la Nación comentado y anotado*, tomo II, 2.ª ed. actualizada y ampliada, 1.ª reimpresión, La Ley, Buenos Aires, 2011 [2004], p. 575; GOTTHEIL/LÓPEZ, *Revista de Derecho Penal y Procesal Penal*, 2004, p. 734; BUOMPADRE, "Estafas y otras defraudaciones" en BAIGÚN (Dir.)/ZAFFARONI (Dir.)/TERRAGNI (Coord.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, t. 7, Hammurabi, Buenos Aires, 2009, pp. 266 y 268; entre otros. DONNA descarta que la extracción de dinero de un cajero automático configure una defraudación en tanto sostiene que la posibilidad de cometer el fraude por medio de una operación automática se encuentra limitada, por concesión del legislador, al supuesto del uso no autorizado de los datos de una tarjeta. En cambio, considera que "[c]uando se trata con medios mecánicos, no hay posibilidad de fraude, porque no hay persona engañada, de modo que […] se trata, cuando hay daño patrimonial, de un hurto" (DONNA, *Delitos contra la propiedad*, 3.ª ed. ampliada, Santa Fe, Rubinzal-Culzoni, 2016 [2001], pp. 589/591).

engañada realice una disposición patrimonial, estimo que las defraudaciones del artículo 173, inciso 15, de dicho ordenamiento, no exigen necesariamente dicha secuencia y toleran, en cambio, otras variantes. Así, puede ocurrir que el error de la víctima se produzca al entregar la información de su tarjeta bancaria -por ejemplo, al autor del *phishing*-, mas el perjuicio patrimonial que la afecta se concrete con posterioridad en un cajero automático o en un local comercial. En segundo lugar, comparto la idea de que todo el que se vea perjudicado patrimonialmente por el uso de la tarjeta de origen ilícito o sus datos (v.gr., propietario del comercio, entidad emisora, titular de la tarjeta) puede ser sujeto pasivo de estos fraudes[15]. En este último sentido, se sostiene: "frente al supuesto en que el sujeto activo realice una operación en un comercio mediante una tarjeta de compra, débito o crédito, perdida, hurtada, robada, etc., y no se pueda determinar de manera documental el fraude frente al comerciante -debiendo hacerse responsable económicamente el titular de la tarjeta- parece claro que el sujeto pasivo es este último, pese a no haber participado de la operación ni haber efectuado él personalmente la disposición patrimonial perjudicial. Lo mismo puede ocurrir en las operaciones de extracción o pago mediante cajeros automáticos"[16]. Entonces, volviendo sobre el ejemplo presentado, puede darse que la víctima sea efectivamente el titular de la tarjeta, que entregó por error sus datos, pero que el engaño que da lugar a la disposición patrimonial -y, por ende, el que es típico del fraude- recaiga sobre un tercero (v.gr., el empleado del local comercial ante quien el autor del hecho presenta la tarjeta apócrifa). A su vez, puede ocurrir que quien captó los datos luego confeccione un plástico falso y extraiga dinero de un cajero automático pero que ello no sea advertido por el titular de la cuenta, caso en el cual también resultaría damnificado, aunque no hubiera hecho la disposición patrimonial. Desarrollaré estas cuestiones más adelante (capítulo IV).

Ahora bien, tal como se adelantó, la defraudación especial del artículo 173, inciso 15, del Código Penal, es la que, en principio, mejor explica los perjuicios patrimoniales producidos mediante las modalidades de captación no autorizada de datos descriptas en los párrafos precedentes, cuando la información obtenida -y luego utilizada- es la de

[15] D'ALESSIO (Dir.)/DIVITO (Coord.), *Código Penal de la Nación comentado y anotado*, tomo II, 2011 [2004], p. 747. De la misma opinión, DONNA, *Delitos contra la propiedad*, 2016 [2001], p. 591 (sin embargo, como se advirtió, este autor no considera que la extracción de dinero de un cajero automático se encuentre incluida en el artículo 173, inciso 15, C.P.).

[16] D'ALESSIO (Dir.)/DIVITO (Coord.), *Código Penal de la Nación comentado y anotado*, tomo II, 2011 [2004], p. 747. Más allá de que en estos casos parece evidente que el titular de la tarjeta resulta damnificado, entiendo que, frente a cualquier supuesto, debe tenerse presente que, según el artículo 2, inciso "a", de la Ley 27.372, se considera víctima a la persona ofendida **directamente** por el delito (el destacado se agregó).

tarjetas de compra, crédito y/o débito[17]. Es que, como se podrá advertir, la figura legal en cuestión abarca tanto el fraude cometido con una tarjeta falsificada como aquel en el que se utilizan solo sus datos. Entonces, se podría válidamente subsumir en el primer supuesto que contempla dicha norma el caso de quien, habiendo obtenido por *skimming* la información de la banda magnética de una tarjeta original, confecciona una apócrifa y la utiliza, por ejemplo, para realizar compras en comercios o extraer dinero de cajeros automáticos. En igual sentido, quedaría incluido en el segundo supuesto el comportamiento de quien realiza compras telefónicas o por Internet con los datos de tarjetas bancarias que obtuvo previamente mediante técnicas de *phishing*, sin que haya existido una interacción física entre dispositivos dispuestos por el autor y las tarjetas. Sin embargo, ambos casos merecen algunas aclaraciones adicionales. En el primero se encuentran en juego distintos tipos penales, por lo que la eventual relación concursal debe ser examinada. Veamos esta cuestión a partir del siguiente ejemplo:

La persona A, empleada de un restaurante, inserta disimuladamente la tarjeta de crédito del cliente B por un *skimmer* al momento de realizar el cobro. Luego, descarga la información captada por su dispositivo y la reproduce en una tarjeta virgen con la que realiza una compra -que es imputada a la cuenta de B- en un local de electrodomésticos.

Tal como se sostuvo precedentemente, el hecho en cuestión podría ser encuadrado válidamente en el primer supuesto del artículo 173, inciso 15, del Código Penal, en tanto A cometió una defraudación con una tarjeta falsificada. Pero para obrar de tal modo debió primero contar con una *lectograbadora* que bien podría ser considerada un instrumento conocidamente destinado a perpetrar una falsificación en los términos del artículo 299 del mismo ordenamiento. En efecto, es a partir de los datos obtenidos con la ayuda de dicho artefacto que A pudo elaborar una tarjeta bancaria apócrifa (art. 282 en función del art. 285 del código sustantivo) y, sobre la forma en la que concurren estos delitos, se ha dicho: "[l]a acción de esta figura [la del art. 299, C.P.] es naturalmente consumida por cualquiera de las penas de la falsificación […] Cuando la falsificación del documento ha tenido comienzo, también desaparece la figura del art. 299"[18]. En este sentido, en el

[17]Mediante el *phishing* se pueden pescar también otros datos -v.gr., claves de acceso a *home banking*- y no solo los de las tarjetas mencionadas. En esos casos (si luego se concreta un daño patrimonial), como se explicará, las opiniones se dividen entre quienes consideran que corresponde aplicar el delito de estafa genérico del artículo 172 del Código Penal, quienes entienden que la maniobra queda abarcada por el fraude informático previsto en el artículo 173, inciso 16, de dicho ordenamiento, y quienes sostienen que la acción es atípica.

[18] SOLER, *Derecho Penal Argentino*, t. V, La Ley, Buenos Aires, 1946, p. 314. En el mismo sentido, D'ALESSIO (Dir.)/DIVITO (Coord.), *Código Penal de la Nación comentado y anotado*, tomo II, 2011 [2004], pp. 1448 y 1528.

ejemplo hipotético, corresponde aplicar las reglas del concurso aparente de leyes y sostener que la falsificación del artículo 282 -en función del artículo 285- del Código Penal desplaza la aplicación de la tenencia del instrumento reconocidamente destinado a cometerla, del artículo 299 de dicho ordenamiento. Es dable mencionar que, si bien algunos autores parecerían aplicar a estos casos el principio de subsidiariedad dado que "hay una *progresión* en la conducta típica, en que la punibilidad de la etapa más avanzada mantiene *interferida* la tipicidad de las etapas anteriores"[19]; otros resolverían la cuestión según la regla de consunción, que solucionaría los llamados actos copenados cuando los hechos están "en una misma línea de progresión en el ataque a un mismo bien jurídico protegido"[20] (en el caso, la tenencia del instrumento sería un acto copenado anterior respecto de la falsificación, en cuyo contenido del ilícito se encuentra incluida).

La relación concursal que media entre la falsificación de la tarjeta (o de un documento de identidad) y la defraudación es más discutida. Mencionaré someramente algunas posturas. Por un lado, se ha sostenido que la falsificación -sea de moneda o de un instrumento público o privado- concurre materialmente con la estafa: "el autor hace dos cosas: primero falsifica o adultera un instrumento y luego defrauda con su uso"[21]. Se trataría, según dicha interpretación, de hechos independientes entre sí (art. 55 del Código Penal). Por otro lado, se considera que, "cuando la estafa se produce mediante la falsificación o el uso de instrumentos que inducen a error a la víctima, provocando un acto de disposición patrimonial perjudicial, esa pluralidad de movimientos voluntarios conforma una única conducta -en los términos del artículo 54 del Código Penal- insusceptible de ser escindida, ya que el segundo tipo se cumple como una forma de

[19] ZAFFARONI/SLOKAR/ALAGIA, *Manual de Derecho Penal: Parte General*, 2.ª ed., 8.ª reimpresión, Ediar, Buenos Aires, 2014 [2005], p. 680.

[20] MUÑOZ CONDE/GARCÍA ARÁN, *Derecho Penal, Parte General*, 9.ª ed., Ed. Tirant lo Blanch, Valencia, 2015 [1993], pp. 505 y 506. A favor de la aplicación del principio de consunción, CÁMARA FEDERAL DE APELACIONES DE SAN MARTÍN, Sala II, Sec. Penal 4, causa n.° 1929, "Incidente de competencia *in re* Giménez s/ inf. art. 282", 15 de mayo de 2001 (cita digital: elDial.com - WS1FA).

[21] NÚÑEZ, *Tratado de Derecho Penal*, t. IV, Ediciones Lerner, Córdoba-Buenos Aires, 1978, pp. 327 y 328. A favor de la existencia de un concurso real entre la falsificación de documento público y la defraudación, CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL FEDERAL, Sala II: "MAZAL, Moisés Raúl y otro", 25 de febrero de 1986; causa n.° 13628, "MAIDANA GONZÁLEZ, I. y otra s/ defraudación", 23 de septiembre de 1997; causa n.° 23110, "SEGOVIA, Walter A. s/ competencia", 20 de septiembre de 2005; causa n.° 23382, "MANRIQUE, Silvia A. s/ competencia", 16 de marzo de 2006; causa n.° 24065, "MAMANI ROJAS, Laureano s/ sobreseimiento", 26 de septiembre de 2006 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 15 de febrero de 2021). En este último, los integrantes del tribunal advierten que, excepcionalmente, algunas falsificaciones pueden concurrir formalmente con la estafa, a cuyo efecto citan el precedente de la CORTE SUPREMA DE JUSTICIA DE LA NACIÓN registrado en Fallos 327:3219, al que haré referencia a continuación.

agotamiento del primero"[22]. En este sentido, se ha dicho que "[s]i el autor de la falsificación de la tarjeta de compra, crédito o débito la utiliza posteriormente para cometer el fraude (art. 173, inc. 15), en ese caso ambas figuras penales concurren de manera ideal, por aplicación de las reglas del concurso previstas por el art. 54 del Código Penal"[23].

Por último, en un fallo ya citado (ver nota al pie n.° 6) en el que el *skimming* se había realizado en un cajero automático, se sostuvo que, como la entidad bancaria era propietaria del *software* de los cajeros, podía haber una violación a sistemas de confidencialidad y seguridad de datos que se debía analizar según las previsiones del artículo157 bis del ordenamiento sustantivo. La falta de argumentación del tribunal en ese sentido impide un mayor análisis, pero, de todas formas, no se advierte que la colocación del dispositivo en la boquilla del cajero automático pueda significar, en los términos de la norma invocada, un acceso ilegítimo -o uno que viola sistemas de confidencialidad y seguridad de datos- a un banco de datos personales.

Ahora bien, la correcta calificación legal del segundo caso -es decir, aquel en el cual un sujeto realiza compras telefónicas o por Internet utilizando datos de tarjetas bancarias previamente pescados mediante técnicas de *phishing*- también merece algunas aclaraciones adicionales. Como se indicó anteriormente, este término se acuña para identificar maniobras cada vez más sofisticadas por medio de las cuales se capta información para una pluralidad de finalidades delictivas (v.gr., extorsionar, estafar, entre otras). Pero no solo pueden ser variadas las finalidades sino también las formas mediante las que se puede procurar alcanzarlas. En su modalidad más frecuente, el primer paso suele presentarse en el envío de correos electrónicos engañosos a partir de los cuales se

[22] Dictamen de la Procuración General de la Nación en S. C. Comp. 1425, L. XLII, "LIMA LOZANO, Ana Claudia s/ denuncia estafa", del 21 de diciembre de 2006, al que la CORTE SUPREMA DE JUSTICIA DE LA NACIÓN hizo remisión en la sentencia n.º 1425 XLII, "LIMA LOZANO, Ana Claudia s/ denuncia estafa", del 6 de marzo de 2007 (Fallos 330:638). En dicho dictamen, a su vez, se hizo referencia al criterio del máximo tribunal en la Competencia n.° 1634, XXXIX, "Jorge Claudio SICA s/ su denuncia s/ infr.art. 292 del C.P.", del 19 de agosto de 2004 (Fallos 327:3219) y la Competencia n.° 630, XLII, "MEYER, Vanesa s/ presunta falsificación de documento público, del 5 de septiembre de 2006. Esta postura fue reiterada por la Corte -haciendo remisión a la opinión de la Procuración General- en: Competencia CSJ 418/2017/CS1, "N.N. s/ falsificación de documentos", 23 de noviembre de 2017; Competencia CCC 52748/2015/3/CS1, "DÍAZ, Miguel y otro s/ falsificación de documentos públicos y uso de documento adulterado o falso (art. 296)", 12 de diciembre de 2017; Competencia CCC 68336/2017/1/CS1, "N.N. s/ falsificación de documentos públicos. Denunciante: SABÁN, Viviana Gloria", 18 de diciembre de 2018; Competencia CSJ 112/2018/CS1, "MASRI, Nicole Sara y/o ROMANOWICZ, Ezequiel Ariel s/ estafa", 14 de agosto de 2018; entre otras. A favor de considerar como supuesto de unidad de acción la utilización de documentos falsos para engañar, RIGHI, *Delito de estafa*, 2017 [2015], p. 187.

[23] ABOSO, *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, reimpr., BdeF, Montevideo-Buenos Aires, 2020 [2017], p. 314.

inicia la comunicación con potenciales víctimas. En dichos *emails*, por ejemplo, el pescador simula pertenecer a una institución bancaria y, mediante un ardid medianamente sofisticado, solicita a los destinatarios sus datos -entre estos, usualmente los de sus tarjetas-. A su vez, puede ocurrir tanto que estos últimos deban aportar información por la misma vía -es decir, simplemente respondiendo el correo electrónico- como que se los redirija a un sitio *web* clonado para que la registren allí. Asimismo, los datos pescados pueden ser los correspondientes a tarjetas bancarias u otros (v.gr., nombres de usuario y contraseñas del servicio de *home banking*). Por lo tanto, se deberá estudiar minuciosamente cada caso concreto para determinar cuál es la subsunción legal adecuada. Sin ánimos de exhaustividad pero sí de tratar los aspectos centrales de la calificación que corresponde asignar a estos comportamientos, valga de disparador el siguiente supuesto hipotético:

La persona A, simulando pertenecer a una empresa de venta de productos tecnológicos, envía correos electrónicos a distintos destinatarios con un enlace a través del cual los invita a acceder al catálogo de ofertas. B ingresa a la supuesta página *web* en la que se ofrecen los productos e intenta comprar uno cargando a tal fin los datos de su tarjeta de crédito (número, fecha de vencimiento, código de seguridad). Estos son recibidos por A, quien luego los utiliza para efectivamente realizar varias compras *online*.

El hecho en cuestión puede ser válidamente subsumido en el tipo penal del artículo 173, inciso 15, segundo supuesto, del Código Penal, pues el autor defraudó mediante el uso no autorizado de los datos de una tarjeta de crédito. Distinta sería la solución si la información que se pescara -y luego aprovechara para obtener beneficios económicos- fuera una clave de acceso al servicio de *home banking*, porque la norma en cuestión prohíbe específicamente el uso no autorizado de datos de tarjetas de compra, crédito o débito, mas no de otros; y, como con razón se sostuvo en doctrina, la aplicación de dicha figura en ese último supuesto vulneraría el principio de legalidad en materia penal "que prohíbe hacer uso de analogías en la adecuación jurídica de conductas"[24]. En virtud de ello, no parece acertada la decisión de calificar como constitutivo de la defraudación del artículo 173, inciso 15, del código sustantivo, el hecho en el cual se utilizan nombres de usuario y contraseñas de *home banking* -captados previamente mediante técnicas de *phishing*- para hacerse abonar ciertas deudas personales desde dichas cuentas[25].

[24] TOSELLI/NICOLOSI LÓPEZ/CHOUELA, *Revista de Derecho Penal y Procesal Penal*, 2007, p. 311.

[25] Contrariamente a lo que se resolvió en CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala VII, causa n.° 27.583, "GERBINO, Venónica Daniela s/ falta

A su vez, frente a casos similares (es decir, aquellos en los que se ingresa a cuentas bancarias y se realizan transferencias a partir de datos pescados mediante técnicas de *phishing*), algunos tribunales se han inclinado por la figura del inciso 16 del artículo 173 del Código Penal[26], en tanto sanciona a quien "defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"[27]. De todos modos, lo cierto es que, al menos en los supuestos mencionados, no parece existir una manipulación informática que *altere* el normal funcionamiento, cuando el legislador prohíbe solo la que es apta para producir dicho efecto[28]. En los casos de *phishing* en los que se utiliza un sitio *web* clonado, se ha advertido que ello "no necesariamente implica, en términos técnicos, alterar ningún funcionamiento ni transmisión de datos, puesto que se realiza un montaje absolutamente nuevo con un único fin defraudatorio. Esto significa que se registra un nuevo dominio de Internet, el que se delega en infraestructura (servidores) implementados a tal efecto y se envían múltiples mensajes, sin usar plataformas de algún modo dañadas, intrusadas o alteradas, sino que se está en presencia de sitios constituidos especialmente con fines defraudatorios o de captación"[29]. Así, "algunos montajes de falsos sitios engañosos no implican más que la creación de algo nuevo, donde no cabría la relación con los conceptos de 'alteración del normal funcionamiento de un sistema' como así tampoco el de la 'transmisión de datos'"[30].

de mérito", 8 de junio de 2016 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020). Corresponde señalar que en el caso se alude, al menos en relación con una de las cuentas bancarias, a una tarjeta de débito, lo que puede haber motivado a que se optara por la calificación legal indicada. Sin embargo, no fueron los datos de dicha tarjeta sino los de acceso a *home banking* los utilizados para defraudar, por lo que el encuadre jurídico parece desacertado.

[26] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.255, "BENTANCOUR, Yesica D. y otros s/ procesamiento", 13 de noviembre de 2018, (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020); Sala VI, causa n.° 39.779, "G. R. y otro s/ procesamientos", 3 de agosto de 2010 (publicado el 14 de septiembre de 2010 en elDial, cita *online* AA62EC).

[27] Artículo 173, inciso 16, del Código Penal, incorporado por el artículo 9 de la Ley 26.388 (Boletín Oficial del 25 de junio de 2008).

[28] PALAZZI, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 3.ª ed., Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2016 [2009], P. 172.

[29] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, 2019, p. 134.

[30] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, 2019, p. 134. En igual sentido, es decir, el de considerar que estos casos de *phishing* no suponen una alteración en los términos de dicha norma, ver PETRONE/BASSO/EMILIOZZI, "*Phishing attacks:* Problemáticas de su recepción en el ordenamiento local y nuevos desafíos", en DUPUY/KIEFER, *Cibercrimen*, t. I, BdeF, Montevideo-Buenos Aires, 2020, pp. 282 y 283.

En este orden de ideas, se ha sostenido que el *phishing* -cuando se verifica un posterior daño patrimonial- queda abarcado por la figura genérica del artículo 172 del Código Penal salvo que tenga por objeto información de tarjetas, en cuyo caso resultaría aplicable la defraudación especial del inciso 15 del artículo 173 de dicho cuerpo normativo[31]. Sin embargo, otros autores han referido -con razón- que no corresponde la subsunción en el tipo penal del mencionado artículo 172 porque, al ser el sujeto activo quien dispone del patrimonio de la víctima, no se encontraría presente el elemento disposición patrimonial exigido en la secuencia de la estafa[32]. En este sentido, además, el artículo 172 del código de fondo no prevé la posibilidad de cometer el hecho mediante una operación automática -como sí lo hace el artículo 173 en su inciso 15-. Entonces, como se podrá advertir, estos casos de *phishing* que no alteran el normal funcionamiento de un sistema informático o la transmisión de datos y recaen sobre información distinta a la de tarjetas bancarias, parecen no tener una respuesta penal clara en nuestra legislación.

Retomando el ejemplo hipotético presentado, es de mencionar que el autor no simuló pertenecer a una empresa real y formalmente registrada, sino a una de venta de productos tecnológicos ficticia. De lo contrario, podríamos encontrarnos frente a una infracción a la Ley de Marcas y Designaciones (art. 31, incisos "a" y "b", Ley 22.362).

Por último, es dable señalar que, en los supuestos de *phishing* en cuestión, la obtención ilícita de información no constituye un acceso a un sistema o dato informático en los términos del artículo 153 bis del Código Penal. Por un lado, la forma en la que la víctima -por error- entrega voluntariamente los datos al pescador no es propia del acceso no autorizado -o en exceso de la autorización que se posea- a un sistema o dato informático de acceso restringido, como el que exige dicha norma. Por otro, lo que esta última prohíbe es la entrada a un sistema informático o alguno de sus componentes, mas no el envío de un correo electrónico al mismo, como suele suceder en el *phishing*.

En resumen, si bien se podrá discutir si -cuando se concreta un daño patrimonial- los casos de *phishing* que recaen sobre datos distintos a los pertenecientes a tarjetas bancarias deben ser calificados como constitutivos del delito de estafa genérica del

[31] PALAZZI, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 2016 [2009], p. 174.

[32] VANINETTI/VANINETTI, "Estafa en Internet", en *El Derecho - Diario*, tomo 211, 2005, p. 689 (cita digital ED-DCCLXVII-336, 14 de febrero de 2005). En el mismo sentido, TOSELLI/NICOLOSI LÓPEZ/CHOUELA, *Revista de Derecho Penal y Procesal Penal*, 2007, p. 312. Al respecto, cabe señalar que en la obra de PALAZZI ya citada, el autor hace referencia a esta publicación de TOSELLI, NICOLOSI LÓPEZ y CHOUELA -y a otra de distintos autores- para sostener: "[e]l caso de ingeniería social, en especial el de phishing, queda abarcado por la figura genérica del art. 172, Cód. Penal, **como ya ha concluido la doctrina**" (ver p. 174 de dicho libro, el destacado se agregó); cuando, al menos según mi interpretación, esos autores parecen concluir lo contrario.

artículo 172 del Código Penal (por lo argumentado precedentemente, creo que esta subsunción es incorrecta), se encuentra fuera de debate que cuando la información pescada y luego utilizada es precisamente la de dichas tarjetas, es el tipo penal del artículo 173, inciso 15, del mismo ordenamiento, el que corresponde aplicar.

Ahora bien, habiendo realizado este análisis sobre la calificación legal que se debe asignar a los supuestos descriptos en los párrafos precedentes, en los que se concretó un perjuicio patrimonial, cabe preguntarse por la incidencia que dichas maniobras de captación de información tienen en el *iter criminis* de los posteriores fraudes cometidos mediante tarjetas falsificadas o el uso no autorizado de sus datos. A modo de ejemplo, ¿qué encuadre jurídico corresponde asignar si una persona es detenida por las fuerzas policiales tras captar la información en cuestión mediante técnicas de *skimming* o *phishing* si aún no utilizó esos datos para defraudar? ¿Ha comenzado en tales casos a cometerse una defraudación y, por ende, nos encontramos frente a un delito tentado, o es que acaso dichos comportamientos constituyen meros actos preparatorios?

III. El comienzo de ejecución en la tentativa de defraudación cometida mediante tarjeta falsificada o el uso no autorizado de sus datos

La distinción entre actos preparatorios y de ejecución de delitos no es una tarea sencilla. Por el contrario, es un tema que ha consumido buenas cantidades de tinta en doctrina y jurisprudencia a lo largo de los años pero que aún no se puede considerar resuelto. Es importante a tal fin la determinación del tipo penal en el que una conducta debe ser encuadrada pues, como se verá, esta es una cuestión a tener en cuenta a la hora de afrontar la difícil asignatura de delimitar el comienzo de la tentativa (en función de ello es que se ha optado por ubicar este capítulo inmediatamente después del correspondiente a la calificación legal).

Ahora bien, dado que al regular la tentativa nuestro Código Penal se refiere expresamente al comienzo de ejecución mas no establece con precisión cuándo esta efectivamente comienza[33], y que no existe consenso acerca de cuál es la teoría que mejor

[33] El artículo 42 de nuestro ordenamiento sustantivo dispone: "[e]l que con el fin de cometer un delito determinado comienza su ejecución…". Aunque no es fácil que una disposición normativa pueda solucionar en pocas palabras lo que la doctrina no ha logrado resolver acabadamente tras largos años de discusión, es posible encontrar en el derecho comparado normas que brindan al intérprete un marco más preciso sobre cuándo comienza la tentativa. A modo de ejemplo, según el §22 del Código Penal alemán "[c]omete tentativa de un delito el que, según su representación del hecho, se pone inmediatamente a realizar el tipo" (traducción de Marcelo A. SANCINETTI en FRISTER, *Derecho Penal. Parte General*, 4.ª ed., 1.ª reimpr., Hammurabi, Buenos Aires, 2016 [2006], p. 463); el artículo 27 del Código Penal colombiano se refiere al que "iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente

resuelve la delimitación entre actos preparatorios y ejecutivos, considero prudente empezar con una breve síntesis de las principales corrientes doctrinarias desarrolladas en la materia, antes de adentrarme específicamente en el estudio de la incidencia que los supuestos de captación ilegítima de datos tienen, a la luz de dichos criterios, en el *iter criminis* de la defraudación. Al respecto, en tanto este no es un trabajo sobre la dogmática de la tentativa en sí, sino más bien uno en el que se pretende analizar, a partir de cuestiones vinculadas a esta última, un tema de la Parte Especial, no realizaré un exhaustivo desarrollo histórico de todas las teorías existentes; por el contrario, me limitaré a abordar sintéticamente tanto las que han tenido mayor acogida en doctrina y jurisprudencia como las que, aunque no con la misma vigencia, resultan necesarias para comprender el porqué de criterios que sí son utilizados en la actualidad.

A. La delimitación entre actos preparatorios y ejecutivos según la doctrina

1. Teoría formal-objetiva[34]

Según esta teoría, la tentativa "comenzaría con el *inicio de la acción descrita en el tipo en sentido estricto*"[35]. Así, en términos del Tribunal Supremo del Reich -que, como explica ROXIN, había reflejado esta idea en su jurisprudencia-, "[l]a tentativa comienza con la acción de ejecución, esto es, con la conducta del autor que desde el punto de vista conceptual cae, en tanto que típica, dentro del tipo del delito…"[36]. Entonces, por poner algunos ejemplos, la ejecución del homicidio empezaría cuando se comienza a matar y la de la estafa cuando se comienza a defraudar (verbos empleados en los tipos penales de los arts. 79 y 172 del Código Penal, respectivamente).

Es precisamente por el apego al contenido literal de la materia de prohibición que se le reconoce a esta teoría la virtud de respetar al máximo el principio de legalidad. Sin embargo, se le critica -entre otras cuestiones- el "no elaborar una pauta o regla racional

dirigidos a su consumación…"; el artículo 24 del Código Penal costarricense establece que "[h]ay tentativa cuando se inicia la ejecución de un delito, por actos directamente encaminados a su consumación…"; el artículo 16 del Código Penal español dispone que "[h]ay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían producir el resultado…".

[34] La teoría formal-objetiva fue obra de BELING y fue sostenida en el país por SOLER (PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 2.ª ed., Hammurabi, Buenos Aires, 1998 [1987], p. 41).

[35] MIR PUIG, *Derecho Penal. Parte General*, 10.ª ed., BdeF, Montevideo-Buenos Aires, 2016 [1984], p. 356.

[36] ROXIN, *Derecho Penal Parte General* (traducción de Diego-Manuel LUZÓN PEÑA, Miguel DÍAZ Y GARCÍA CONLLEDO, José Manuel PAREDES CASTAÑÓN, Javier de VICENTE REMESAL y otros), t. II, 3.ª reimpr., Thomson Reuters-Civitas, Buenos Aires, 2019 [2014], p. 467, citando RGSt [Sentencias del Tribunal Supremo del Reich en asuntos penales] 70, 151 (157/58).

más concreta para determinar en forma específica el límite entre lo punible y lo impune"[37], pues "remitir al comienzo de la acción típica para resolver cuándo se comienza la ejecución típica encierra una tautología que no ofrece ningún criterio útil […] ¿cuándo comienza la acción de matar? ¿al sacar la pistola, al apuntar, al apretar el gatillo?"[38]. Y responder estas inquietudes desemboca en una posible segunda objeción a las ideas de BELING, cual es la de la estrechez al delimitar los actos preparatorios de los ejecutivos por la que se excluirían incorrectamente de la tentativa acciones inmediatamente anteriores a la realización de la conducta típica. Nótese que, con este razonamiento, se debería sostener que no inicia la ejecución de un abuso sexual quien ejerce violencia contra la víctima si aún no empezó a abusar (art. 119 del ordenamiento sustantivo), lo que no parece razonable. Como señala ROXIN al analizar a modo de ejemplo la figura del §212 del Código Penal alemán, "el disparo del revólver se entendería, en tanto verdadera acción de homicidio, como tentativa, pero no preparar el arma o apuntar con ella; pues estos actos preceden a la acción típica"[39]. De hecho, bajo una aplicación estricta de esta teoría, se debería incluso concluir que los delitos de acción instantánea como el homicidio no admitirían por regla el conato, "puesto que el verbo típico <<matar>> no puede realizarse parcialmente: se mata o no se mata"[40].

En función de estas consideraciones es que se sostiene que la teoría formal-objetiva debería partir "de un entendimiento de la acción típica en sentido amplio, más amplio que el de su estricta realización"[41]. Pero aun bajo esta perspectiva subsiste la crítica a su carencia de criterio con el cual marcar un límite sin necesidad de remitir al verbo típico.

2. Teoría material-objetiva

Esta variante intenta corregir la teoría objetivo-formal apelando a criterios materiales que permitan, también objetivamente, abarcar en el comienzo de la acción típica el campo previo a la consumación.

En este sentido, significó una primera aproximación a ese fin la fórmula de FRANK de la concepción natural, conforme a la cual "son ejecutivos los actos que se hallan de tal

[37] PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 43.
[38] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 356.
[39] ROXIN, *Derecho Penal Parte General*, 2019 [2014], p. 467.
[40] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 357.
[41] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 357.

forma unidos a la acción típica, que según la concepción natural aparecen como *parte suya*"[42]. Pero esta idea fue también motivo de objeciones, en particular, por su imprecisión y vaguedad a la hora de explicar cuándo una conducta tiene una necesaria vinculación con la acción típica según esa concepción natural. Porque, aunque se guíe acertadamente por una perspectiva de proximidad al tipo, deja librada a un juicio intuitivo la cuestión de qué acciones anteriores a este pertenecen ya a la tentativa[43]. Tampoco se concreta cuál es el límite hasta el que se extendería "hacia atrás" -temporalmente hablando- la ejecución típica y, "al no establecerse límite alguno, otra vez el fantasma de la inseguridad jurídica asoma su peligroso rostro"[44].

Una alternativa pretende concretar esa imprecisión recurriendo a la noción de peligro. Así, "habrá tentativa cuando se pone en peligro el bien jurídico"[45]. Pero, como se podrá advertir, a este criterio le cabe la misma crítica que al que intenta solucionar, pues "siempre será discutible cuándo empieza a producirse una puesta en peligro inmediata"[46]. En este sentido, no queda claro "cuál es la pauta sobre la que se afirma la existencia o ausencia de peligro"[47].

3. Teoría objetiva-individual[48]

Según esta teoría, "la tentativa comienza con aquella actividad con la cual el autor, según su plan delictivo, se pone en relación inmediata con la realización del tipo

[42] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 357, con cita a FRANK, *Strafgesetzbuch* §43, II, 2b (ver nota al pie n.° 41 de la obra citada).
[43] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 477.
[44] PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 46. También críticos de la imprecisión de la fórmula de FRANK se expresan ZAFFARONI/ALAGIA/SLOKAR, *Manual de Derecho Penal: Parte General*, 2014 [2005], p. 647; y MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 357.
[45] PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 46. Como reseña este autor, SCHÖNKE y SCHRÖDER hablan del "peligro inmediato" (ver nota al pie n.° 27 de la página 45 de su obra aquí citada).
[46] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 358.
[47] PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 47.
[48] Esta teoría, también llamada *Teoría del plan concreto del autor*, fue desarrollada por WELZEL y seguida en nuestro país, entre otros juristas, por ZAFFARONI. Es dable señalar que PESSOA, sobre la base de las ideas de WELZEL, ha elaborado el criterio del llamado acto productor de la finalidad para la delimitación del principio de ejecución. En prieta síntesis, de la cadena de comportamientos -unidos por una finalidad- que el autor del hecho realiza, PESSOA distingue -desde una perspectiva de tipo funcional- entre los actos pensados con la tarea de materializar esa finalidad y los que fueron pensados para posibilitarlos. Así, el "*acto productor de la finalidad* es el acto de tentativa" y el "acto posibilitador del productor de la finalidad es el acto preparatorio" (PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 73).

delictivo"[49]. Se parte de la idea de que el comienzo de la ejecución de un delito no puede determinarse en abstracto sino solo con relación a un proyecto de acción en concreto. De este modo, se explica: "[s]i de lo que se trata es de abarcar en el comienzo de ejecución la acción inmediatamente anterior a la del verbo típico en sí mismo, es decir, la que no presenta posibilidad alguna de interposición de otra acción que no sea la de la teoría formal objetiva, esto no puede hacerse en abstracto, sino en concreto, es decir, tomando en cuenta el *cómo* de la realización del verbo típico. Este *cómo* es el *plan concreto del autor*"[50]. Entonces, la distinción entre actos preparatorios y de ejecución se realiza acudiendo a un aspecto subjetivo (el plan del autor) y a uno objetivo (la acción cumplida). En resumen, "(a) el comienzo de ejecución del delito no es estrictamente el comienzo de ejecución de la acción señalada objetivamente por el verbo típico, (b) sino que también abarca los actos que, conforme al plan del autor […], son inmediatamente anteriores al comienzo de la ejecución de la acción típica e importan objetivamente un peligro para el bien jurídico, bien entendido que (c) un acto parcial será inmediatamente precedente de la realización de la acción típica cuando entre ésta y aquél no haya otro acto parcial en el plan concreto del autor"[51].

Al igual que las anteriormente sintetizadas, esta teoría es también merecedora de objeciones pues "contiene todavía un considerable margen de imprecisión, de elasticidad en el mismo sentido o del mismo tipo que la que atribuimos a otras teorías, aunque en menor magnitud"[52]. Por cierto, esta es una cuestión que algunos de sus propios defensores reconocen al aclarar que "el criterio objetivo individual tampoco proporciona una regla del todo cierta para señalar el límite preciso entre los actos preparatorios y los de tentativa", aunque entienden que "en tanto la dogmática penal no disponga de bases más certeras, en los casos en que la duda aparezca insalvable, lo correcto es apelar a la interpretación restrictiva de la ley"[53].

4. Teoría de los actos parciales, concretada

Bajo este mismo título ROXIN explica la concepción que entiende adecuada para delimitar el comienzo de la tentativa. Como se verá, este autor parte de criterios rectores

[49] WELZEL, *Derecho penal alemán. Parte general* (trad. Juan BUSTOS RAMÍREZ y Sergio YAÑÉZ PERES), 11.ª ed. (4.ª ed. en español), Editorial Jurídica de Chile, Santiago, 1970, p. 283.
[50] ZAFFARONI/ALAGIA/SLOKAR, *Manual de Derecho Penal: Parte General*, 2014 [2005], p. 648.
[51] ZAFFARONI/ALAGIA/SLOKAR, *Manual de Derecho Penal: Parte General*, 2014 [2005], pp. 649 y 650.
[52] PESSOA, *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 1998 [1987], p. 50.
[53] ZAFFARONI/ALAGIA/SLOKAR, *Manual de Derecho Penal: Parte General*, 2014 [2005], p. 649.

seguidos por teorías desarrolladas precedentemente -por ejemplo, la proximidad al tipo en la fórmula de FRANK- para concretarlos a través de los conceptos auxiliares de conexión temporal estricta e incidencia sobre la esfera de la víctima o del tipo[54].

En primer lugar, según este razonamiento, la proximidad al tipo funciona como criterio guía para determinar el comienzo de la tentativa. No se trata de "un elemento del que sea posible deducir inmediatamente conclusiones válidas para el caso concreto"[55], sino más bien de "un criterio supremo, de un punto de vista orientador, que ha de ser concretado en relación con la materia a regular"[56].

En segundo lugar, así como ROXIN reconoce virtudes a la fórmula de FRANK, también considera como uno de los intentos de delimitación relativamente más afortunados el realizado por la teoría de los actos parciales, que "vincula el comienzo de la tentativa al último acto parcial antes de la verdadera acción típica; tras la entrada en la fase de tentativa no tiene lugar ningún 'acto intermedio' más, sino que la siguiente acción es ya aquella que desencadena el resultado"[57]. El problema que tiene esta concepción, pese a permitir una delimitación precisa por tener en cuenta cada movimiento corporal como acto intermedio, es que acaba por hacerla depender "de forma poco convincente del azar de la configuración externa de la acción"[58]. Adviértase que, de este modo, "[e]xistiría tentativa en extender la mano hacia el objeto que se pretende robar; la apertura del cajón en el que éste se halla sería mera preparación, pues otro acto intermedio tendrá lugar antes del apoderamiento"[59].

Para evitar una perspectiva que haga la división estrictamente conforme a los movimientos corporales, los defensores de dicha teoría exigen, entonces, que entre el inicio de la tentativa y la acción típica "no concurra ningún acto parcial **esencial** más"[60]. Sin embargo, determinar esa esencialidad resulta ser una cuestión de valoración que, en definitiva, despoja a esta fórmula de su precisión[61]. Además, al alejarse de una división

[54] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 479 y ss.
[55] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 466.
[56] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 466.
[57] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], pp. 474 y 475.
[58] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 478.
[59] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 478.
[60] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 478, con cita a RUDOLPHI, fundador de la teoría de los actos parciales (ver nota al pie n.º 150 de la obra citada).
[61] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 479.

según movimientos corporales singulares, "la solución del acto parcial pierde su estricta sujeción al tipo"[62].

En este orden de ideas, ante la necesidad de concretar la teoría de los actos intermedios, ROXIN sostiene que "el último bloque de acto parcial debe ser descrito a través de los conceptos auxiliares de **'conexión temporal estricta'** y de **'incidencia sobre la esfera de la víctima o del tipo'**"[63]. Si estos concurren conjuntamente, habrá comenzado la tentativa. Por el contrario, serán actos preparatorios aquellos en los que estos no se encuentren presentes. Para la conexión temporal estricta "hay que observar que la misma debe concurrir en relación con la acción típica, pero no necesariamente respecto del resultado […] Debe concurrir, no obstante, una conexión con el resultado en aquellos casos en los que, según el plan del autor, aquél debería seguir de manera ininterrumpida"[64]. Con respecto al segundo concepto auxiliar, "[a]llí donde falte una 'esfera' especial en el lado del atacado, se debe tomar como punto de referencia la esfera del tipo"[65].

B. *Skimming*, *phishing* y el comienzo de la tentativa de defraudación según la jurisprudencia

A pesar de las limitaciones vinculadas a la determinación del comienzo de ejecución ya señaladas (la falta de precisión en el Código Penal y de consenso en la doctrina), los criterios reseñados precedentemente resultan de gran utilidad al tener que resolver, en un caso concreto, si un acto es preparatorio o ejecutivo respecto de un determinado delito como, en lo que aquí interesa, si la captación ilegítima de datos de tarjetas bancarias mediante *skimming* o *phishing* configura o no el inicio de la tentativa de las defraudaciones previstas en el artículo 173, inciso 15, del ordenamiento sustantivo. En similar sentido, a los fines de dicho análisis, es ilustrativo detenerse en cómo se ha interpretado esta cuestión en la jurisprudencia, donde muchos parecen aceptar que las maniobras fraudulentas cometidas con tarjetas bancarias tienen el principio de ejecución

---

[62] JAKOBS, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación* (trad. Joaquín CUELLO CONTRERAS y José Luis SERRANO GONZÁLEZ DE MURILLO), 2.ª ed. corregida, Marcial Pons, Madrid, 1997 [1983], p. 883.

[63] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 479. Tal como señala el autor, la utilidad de estos dos criterios es reconocida frecuentemente por la doctrina (ver nota al pie n.° 155 en la p. 480). Así, por ejemplo, JAKOBS considera la "proximidad temporal" y la "irrupción del autor en la esfera de protección del atacado" como directrices positivas (también formula otras negativas) que orientan la decisión sobre el comienzo de la tentativa (JAKOBS, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación*, 1997 [1983], pp. 884 y 886).

[64] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 481.

[65] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 481.

en las conductas dirigidas a la obtención de sus datos, independientemente de si se encuentra corroborada o no la acción por la que se busca conseguir el beneficio patrimonial (v.gr., la presentación de la tarjeta falsificada en un local para realizar una compra, su uso en un cajero automático para extraer dinero, etcétera).

Así, por ejemplo, frente a un caso en el que se colocó un dispositivo, conectado a una laptop, en la boquilla lectora de un cajero automático para copiar datos de tarjetas de crédito y débito y así proceder a su posterior duplicación, se consideró que se encontraba configurado el delito de tenencia de instrumentos destinados a la falsificación en concurso material con tentativa de defraudación en tanto, "[a]un cuando no se haya acreditado la existencia de movimientos no autorizados en las cuentas individualizadas, el mecanismo era idóneo para cometer una defraudación (art. 173, inc. 15° del C.P.)"[66]. Sin perjuicio de la relación concursal escogida (al respecto, ver las distintas posturas explicadas en el apartado B del capítulo II), en el caso se puede ver con claridad que lo determinante para esos magistrados fue la idoneidad del medio para cometer el fraude. Nótese que, tal como surge del fallo, no se habían constatado conductas directamente dirigidas a obtener un beneficio patrimonial y que perjudicaran a terceros. De este modo, no se atendieron cuestiones como si el comportamiento significaba el comienzo de la ejecución de la acción de defraudar o una inmediata puesta en peligro a la propiedad; tampoco si, según el plan del autor, existían otros actos a realizar antes del correspondiente al verbo típico o si se presentaba la conexión temporal que, como vimos, exige gran parte de la doctrina.

En un caso no ya de pescadores de datos sino de tarjetas físicas, es decir, supuestos en los cuales los autores intentan -mediante un dispositivo y algún ardid- hacerse del plástico original para luego utilizarlo y obtener un beneficio patrimonial, otra sala del mismo tribunal abonó la postura de que ello ya resultaba típico del fraude. En este sentido, uno de los magistrados intervinientes sostuvo que "'la mise en scène' montada reúne, por sus características, la aptitud necesaria para provocar error en la víctima y, en consecuencia, la subsunción típica que corresponde asignar a la conducta en estudio tendría como base alguna de las defraudaciones contempladas por el artículo 172 y siguientes del Código Penal"[67]. El otro señaló que "además del emplazamiento del

[66] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala VI, causa n.° 26.683, "CASTELLINI, Alfredo José y otros", 30 de marzo de 2005, voto de los jueces BUNGE CAMPOS, ESCOBAR y GEROME (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020).

[67] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 1365, "CAMPOS, Liliana G.", 11 de octubre de 2011, voto del juez LUCINI (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

dispositivo aludido como 'pescador', la imputada […] entabló contacto personal con aquélla [la víctima] en orden a concretar la maniobra por la cual pretendía obtener dinero, de lo que se colige la existencia de un ardid o engaño típico de la figura prevista en el artículo 173, inciso 15°, del Código Penal"[68]. Es dable aclarar que, aunque se trate de casos en los que se pretende obtener la tarjeta física -y, quizá, también una clave de acceso-, los argumentos no dejan de resultar útiles para los supuestos en los que se capta exclusivamente información, puesto que esta defraudación puede ser cometida tanto mediante una tarjeta falsificada como hurtada y/o sus datos. Por cierto, como se verá más adelante, frente a plataformas fácticas análogas, otros jueces del mismo tribunal entendieron que en esos casos la ejecución del fraude no se encontraba iniciada.

Es criterio de la Corte Federal y de la Procuración General de la Nación que la defraudación cometida con tarjetas comienza con las maniobras engañosas dirigidas a la obtención de sus datos. En este sentido, en un supuesto en el que se investigaban las conductas realizadas por una persona que solicitaba datos de tarjetas bancarias a empleados de una estación de servicio para luego conseguir beneficios económicos con estos, el máximo tribunal hizo remisión al dictamen del representante del Ministerio Público Fiscal quien, a su vez, sostuvo que "la maniobra defraudatoria habría tenido comienzo de ejecución en jurisdicción de San Isidro, con el despliegue engañoso dirigido a la obtención de los datos de las tarjetas de compra"[69]. Claro está, la modalidad utilizada para captar la información de los plásticos fue distinta a las aquí analizadas, pero la doctrina de dicho precedente fue reiterada invariablemente por la Corte desde ese entonces hasta la actualidad, independientemente de las maniobras escogidas a dicho fin[70]. Tanto es así que, en supuestos análogos y fechas recientes, el tribunal cimero

[68] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 1365, "CAMPOS, Liliana G.", 11 de octubre de 2011, voto del juez CICCIARO (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

[69] Dictamen del Procurador General de la Nación en S. C. Comp. 1249, L. XLI, "LÓPEZ, Santiago Alberto s/ delito de acción pública", del 14 de septiembre de 2005, al que la CORTE SUPREMA DE JUSTICIA DE LA NACIÓN hizo remisión en la sentencia n.º 1249 L. XLI, "LÓPEZ, Santiago Alberto s/ delito de acción pública", del 20 de diciembre de 2005.

[70] C.S.J.N.: C. 1355. XLI, "LÓPEZ, Santiago Alberto s/estafa", del 20 de diciembre de 2005; C. 151. XLIV, "LÓPEZ, Santiago Alberto s/ denuncia", del 29 de abril de 2008; C. 546. XLIV, "Droguería del Sud (personal) y Farmacia Jardín (personal) s/ defraudación", del 10 de marzo de 2009; C. 158. XLVI, "QUIROGA, Valeria Analía s/ su denuncia", del 22 de junio de 2010; C. 403. XLVI, "QUIROGA, Valeria Analía s/ denuncia", del 5 de octubre de 2010; C. 489. XLVI, "QUIROGA, Valeria Analía y otros s/ denuncia", del 2 de noviembre de 2010; C. 704. XLVI, "QUIROGA, Valeria Analía s/ denuncia", del 30 de noviembre de 2010; C. 244. XLVII, "QUIROGA, Valeria Analía s/ denuncia", del 23 de junio de 2011 (Fallos: 334:796); C. 497. L, "RODRÍGUEZ MANCEDIÑO, María Belén s/ su denuncia - defraudación (art. 173 inc. 15)", del 2 de diciembre de 2014; CCC 25393/2014/2/CS1, "N.N. s/ defraudación (art. 173 inc. 15)", del 30 de junio de 2015; CCC 32970/2014/1/CS1, "N.N. s/ defraudación art. 173, inc. 15", del 14 de julio de 2015; CCC 45394/2015/1/CS1, "ENRIQUEZ, María Leandra y otros s/ denuncia", del 22 de

continúa remitiéndose a lo dictaminado por la Procuración General de la Nación, desde donde se sostiene contundentemente que "el Tribunal [la Corte] tiene dicho que la maniobra fraudulenta realizada con una tarjeta tiene principio de ejecución con el despliegue engañoso dirigido a la obtención de sus datos"[71]. Con todo, considero prudente señalar que la intervención de la Corte Federal en los precedentes citados se limitó a la resolución de cuestiones de competencia y, a ese fin, no se realizó un análisis dogmático exhaustivo del tipo penal en estudio. A su vez, en algunos de esos fallos la decisión se apoyó no solo en el argumento sobre el principio de ejecución ya mencionado sino también en otras circunstancias (v.gr., lugar donde se realizaron las compras fraudulentas y/o donde las partes tenían sus domicilios).

En los fallos que se señalan a continuación, en cambio, se pueden apreciar razonamientos según los cuales el comienzo de la defraudación se ubicaría en la realización de conductas que, en concreto, afectan o pueden afectar patrimonios de terceros.

En un precedente de *cloning* o *skimming* bancario ya citado (ver nota al pie n.° 6), la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal debía resolver un recurso contra un sobreseimiento dictado en primera instancia en los términos del artículo 336, inciso 3, del Código Procesal Penal de la Nación, en el entendimiento de que la captación de datos de tarjetas conformaba la etapa de preparación de la defraudación y no su tentativa. El juez de grado, además, argumentaba que no se podía establecer la información almacenada en el dispositivo. En dicha oportunidad no se habían constatado aún perjuicios patrimoniales pero existían

noviembre de 2016; CCC 76398/2015/1/CS1, "LERMAN, Marcelo David y otros s/ su denuncia - defraudación art. 173, inc. 15 del C.P.", del 7 de marzo de 2017; CCC 5390/2016/1/CS1, "LERMAN, Marcelo David y otros s/ su denuncia - defraudación art. 173, inc. 15 del C.P.", del 7 de marzo 2017; CCC 37481/2015/1/CS1, "ENRIQUEZ, María Leandra y otros s/ legajo de apelación", del 21 de marzo 2017; CCC 23455/2016/1/CS1, "Prisma Medios de Pago SA y otros s/ defraudación (art. 173, inc. 15 del C.P.) s/ incidente de competencia", del 21 de marzo de 2017; CCC 39199/2016/1/CS1, "N.N. s/ defraudación (art. 173, inc. 15 del C.P.). Denunciante: LERMAN, Marcelo David y otros", del 15 de agosto de 2017; CCC 37760/2015/1/CS1, "ENRIQUEZ, María Leandra y otros s/ incidente de incompetencia", del 26 de septiembre de 2017; CCC 69533/2016/1/CS1, "N.N. s/ defraudación. Denunciante: LERMAN, Marcelo David y otros", del 26 de diciembre de 2017; CCC 19838/2017/1/CS1, "N.N. s/ defraudación. Denunciante: LERMAN, Marcelo David y otros", del 15 de mayo de 2018; CCC 18683/2017/1/CS1, "N.N. s/ defraudación. Denunciante: LERMAN, Marcelo David y otros", del 15 de febrero de 2018; CCC 63129/2015/1/CS1, "GÓMEZ, Marilyn Noemí s/ defraudación", del 20 de febrero de 2018; CSJ 1620/2019/CS1, "RODRÍGUEZ, Martín s/ estafa", del 17 de septiembre de 2020; FLP 114282/2018/CS1, "GSELL, Miguel Ángel s/ defraudación", del 15 de octubre de 2020 y CSJ 2096/2019/CS1, "N.N. s/ estafa", del 29 de octubre de 2020.

[71] Dictamen del Procurador General de la Nación interino en Comp. CSJ 2096/2019/CS1, "N.N. s/ estafa", del 2 de diciembre de 2019, al que la C.S.J.N. hizo remisión en Competencia CSJ 2096/2019/CS1, "N.N. s/ estafa", del 29 de octubre de 2020.

medidas pendientes que podían corroborar esta cuestión, por lo que los magistrados intervinientes consideraron que la resolución era prematura y la revocaron. Más allá de esta conclusión, la lectura de sus argumentos permite establecer que tuvieron un criterio distinto al que se apuntó en los fallos de párrafos precedentes. Ello en tanto sostuvieron que, como aún se debía corroborar si se habían realizado operaciones en perjuicio de distintos usuarios, no se podía descartar "que la maniobra en ciernes hubiere trascendido el mero estadio de acto preparatorio, conformando principio de ejecución de la conducta defraudatoria con idoneidad para vulnerar el bien jurídico tutelado por la norma"[72], por lo que debían extremarse los recaudos para determinar si había mediado factibilidad de afectación patrimonial en concreto. En este sentido, según dichos jueces, no se podía a esa altura descartar que hubiera comenzado la defraudación (agrego, tampoco afirmarlo) y sí resultaba útil a tal fin constatar si habían existido operaciones que perjudicaran o pudieran perjudicar patrimonialmente a terceros. Entonces, con ese razonamiento, el comienzo de ejecución no estaría ubicado en la maniobra mediante la cual se captan los datos sino en las conductas que, en concreto, pueden afectar patrimonios de terceros. Por cierto, dado que en el caso también se encontraba en discusión la consideración de las figuras de los artículos 285 y 299 del Código Penal, se sostuvo al respecto que "para los casos de copiado de banda magnética, el proceso de falsificación no comienza con la toma de los datos de la tarjeta, circunstancia previa -aunque necesaria- para la posterior hechura de la tarjeta apócrifa, sino en el momento en que estos comienzan a volcarse en un plástico nuevo al que, además se le da la apariencia externa de una tarjeta legítima. En ese sentido, la conducta de quien se encuentra copiando bandas magnéticas por medio de estos dispositivos técnicos resultaría atípica en relación con la figura contemplada por el artículo 285 del C.P., en función del art. 282, sin perjuicio de que, si hay luego comienzo de ejecución, esas conductas pueden ser punibles como participación en el hecho típico"[73].

Tal como se adelantó, en otro supuesto de pesca de tarjetas físicas particularmente similar al ya citado (ver nota al pie n.° 67), la Sala IV de la misma Cámara de Apelaciones -aunque con distinta integración- consideró que "si bien constituye una hipótesis valedera

[72] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.663, "OLIVEIRA RIVAS, Fabio y otros s/ defraudación", 20 de agosto de 2008 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

[73] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.663, "OLIVEIRA RIVAS, Fabio y otros s/ defraudación", 20 de agosto de 2008 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

sostener que la maniobra en cuestión [el autor había colocado en la ranura del cajero automático un dispositivo que retuvo la tarjeta de la víctima y luego aparecido en escena ofreciéndole ayuda, momento en el que fue detenido por fuerzas policiales] habría tenido en miras la obtención de la tarjeta de débito con el fin de llevar a cabo a *posteriori* una operación espuria en un cajero automático, lo cierto es que esta situación ni siquiera aparece iniciada…"[74]. De ese modo, contra lo que alegaba el representante del Ministerio Público Fiscal ante esa instancia, se descartó que hubiera comenzado una defraudación en los términos del artículo 173, inciso 15, del Código Penal y se calificó la conducta como constitutiva de hurto simple en grado de tentativa.

Por otro lado, en un caso de *phishing* -cuya calificación legal aquí se criticó (ver nota al pie n.° 26)- en el que se discutía, entre otras cuestiones, el grado de realización del tipo (en esa oportunidad, si el delito estaba consumado o tentado), se ubicó la tentativa "en la realización de aquellos actos de manipulación informática que no logran el resultado pretendido por causas ajenas a la voluntad del autor"[75]. Se encontraba bajo análisis el accionar de la persona que, habiendo recibido una transferencia bancaria en una cuenta personal desde otra cuyos datos habían sido pescados ilegítimamente, se dirigió al banco a retirar el dinero y no pudo hacerlo porque se le exigió que presentara documentación que acreditara su origen. Aunque es evidente que dicha conducta significaba un grado de realización del tipo más avanzado que el de la mera captación de datos, vale la pena remarcar que el criterio seguido para delimitar la tentativa se acercó más bien al momento en el que se desarrollan las maniobras tendientes a obtener el beneficio patrimonial.

IV. *Skimming* y *phishing*: ¿actos preparatorios o ejecutivos de la defraudación?

Como se habrá podido advertir, pese a que es criterio consolidado de la Corte Suprema de Justicia de la Nación y de otros tribunales que la maniobra fraudulenta realizada con una tarjeta tiene principio de ejecución con las conductas dirigidas a la obtención de sus datos, existen fallos en los cuales se exigen, además, actos dirigidos a conseguir un beneficio económico, más cercanos -temporalmente hablando- a la

[74] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 364, "CÁCERES, María Victoria", 15 de abril de 2011, voto de los jueces SEIJAS y GONZÁLEZ (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

[75] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.255, "BENTANCOUR, Yesica D. y otros s/ procesamiento", 13 de noviembre de 2018 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020).

producción de perjuicios a terceros. Según este último criterio, entonces, la captación no autorizada de información no constituiría el comienzo de la posterior defraudación puesto que no afecta ni podría afectar por sí sola el patrimonio de otro.

Habiéndose repasado los principales fundamentos jurisprudenciales vinculados al tema en estudio, podemos volcarnos al análisis de la incidencia que las maniobras de captación de información tienen en las defraudaciones cometidas mediante tarjetas falsificadas o el uso no autorizado de sus datos. Al efecto, hace algunos instantes se presentaban los siguientes interrogantes: ¿qué calificación legal corresponde asignar si una persona es detenida por las fuerzas policiales tras captar información de tarjetas de crédito y/o débito mediante técnicas de *skimming* o *phishing* si aún no utilizó esos datos para defraudar? ¿Ha comenzado en tales casos a cometerse una defraudación y, por ende, nos encontramos frente a un delito tentado, o es que acaso dichos comportamientos constituyen meros actos preparatorios?

Es claro que las circunstancias particulares de cada supuesto de hecho serán determinantes para responder estas preguntas pues, como se dijo, la decisión sobre el inicio de la tentativa no se debe tomar en abstracto sino en función de un proyecto de acción que se exterioriza. De este modo, habrán de tenerse en cuenta cuestiones relevantes como, por ejemplo, si el autor ya colocó el dispositivo en la ranura del cajero automático en un caso de *skimming*, si descargó o no los datos registrados por la *lectograbadora*, si los volcó en una tarjeta apócrifa, si entregó esta última al empleado de un local para efectuar una compra o solo merodea con ella por dicho comercio, si la insertó en un cajero automático, si ofreció y/o vendió la información a un tercero, etcétera. En similar sentido, se deberá constatar en un supuesto de *phishing* si el pescador envió los correos electrónicos para pescar los datos de sus destinatarios, si estos últimos efectivamente los aportaron, si el autor los cargó en un sitio *web* para realizar una compra *online*, si se los proporcionó telefónicamente a un empleado para adquirir un bien o servicio, si los ofreció y/o vendió a otro, etcétera. Como se podrá advertir, son muchas las circunstancias a considerar a la hora de calificar jurídicamente estos casos y, a tal fin, determinar si se ha alcanzado un grado de realización del hecho que permita concluir que comenzó la tentativa. Es precisamente para esta tarea que cobran vital relevancia los criterios desarrollados por la doctrina, reseñados en el apartado A del capítulo III.

Ahora bien, dada la multiplicidad de supuestos de hecho que se pueden presentar en la práctica y por una cuestión de claridad expositiva, propongo ordenar el análisis en grupos de casos en los que se encuentren abarcados los distintos actos dirigidos a cometer,

mediante *skimming* o *phishing*, una defraudación en los términos del artículo 173, inciso 15, del Código Penal. En este sentido, ya que el presente trabajo no busca identificar de modo genérico cuál es el comienzo de la tentativa de estos casos especiales de estafa sino determinar si dichas modalidades de obtención no autorizada de datos en particular configuran o no el principio de su ejecución, el estudio se dividirá en dos grandes momentos que conforman estos supuestos de captación ilegítima de información.

Así, se analizará en primer lugar la conducta de instalar el dispositivo en la ranura del cajero automático en un caso de *skimming* o enviar los correos electrónicos engañosos en uno de *phishing*; es decir, aquellos actos que el autor realiza y luego de los cuales solo debe esperar los aportes de las víctimas -que inserten sus tarjetas en el cajero o respondan el correo recibido-. En segundo lugar, se estudiará el hecho por el que el sujeto activo concreta la obtención de información: retira el aparato del cajero, recibe los *emails* de sus destinatarios, descarga los datos captados…, en suma, comportamientos a partir de los cuales el autor ya dispone efectivamente de ellos para concretar el fraude de acuerdo a su plan delictivo. Por último, se examinarán algunas acciones que podrían suceder a la pesca de datos como, por ejemplo, volcarlos en una tarjeta virgen e, incluso, desistir del plan y, en cambio, vender la información obtenida.

A. Análisis de casos

1. El autor coloca el dispositivo en la ranura del cajero automático o envía correos electrónicos engañosos para pescar datos

Como ya se señaló, los supuestos más comunes de *skimming* o *cloning* bancario comienzan con el acto por medio del cual el autor del hecho, de manera disimulada, coloca en la boquilla de un cajero automático la *lectograbadora* que registrará la información de las tarjetas que allí se inserten -en ocasiones acompañada de una pequeña cámara-. Se trata de casos en los que el autor ya dio un primer paso y solo debe esperar a que las potenciales víctimas introduzcan sus tarjetas para luego retirar el artefacto. Entonces tendrá a su disposición los datos y podrá utilizarlos para llevar adelante el fraude.

Así planteado el caso, la mera colocación del dispositivo en el cajero automático resultaría similar al envío de correos electrónicos engañosos en el *phishing*. Es decir, se trataría de dos supuestos en los cuales el autor ya llevó a cabo un primer acto dirigido a la obtención de información, exteriorizó lo que hasta entonces solo era un plan delictivo y debe esperar el aporte de terceros -que inserten sus tarjetas en el cajero automático que

tiene el *skimmer* instalado o aporten los datos vía correo electrónico-. Claro está, la analogía se daría solo en los hechos pues, como se verá, la calificación legal sería distinta en uno y otro caso.

En este orden de ideas y a modo ilustrativo, se podría ubicar en este grupo el fallo de la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional ya citado, en el que se encontraba bajo análisis el accionar de quien colocó un dispositivo, conectado a una laptop, en la boquilla lectora de un cajero automático para copiar datos de tarjetas y así proceder a su posterior duplicación. Como se mencionó, en dicha oportunidad se consideró que se encontraba configurado el delito de tenencia de instrumentos destinados a la falsificación en concurso material con tentativa de defraudación en tanto, "[a]un cuando no se haya acreditado la existencia de movimientos no autorizados en las cuentas individualizadas, el mecanismo era idóneo para cometer una defraudación (art. 173, inc. 15° del C.P.)"[76]. También se podrían incluir los casos de los pescadores de tarjetas ya mencionados, dado que son supuestos en los que los autores, mediante la instalación de un aparato en el cajero, buscan apropiarse de los plásticos. La diferencia solo estribaría en que en un hecho se procura obtener datos y en el otro directamente tarjetas[77].

Ahora bien, en este y otros casos en los que el autor únicamente instala el dispositivo para captar información -o incluso tarjetas físicas-, resulta evidente que, a los fines de la materia de prohibición definida en el artículo 173, inciso 15, del ordenamiento sustantivo, la acción no se encuentra iniciada. La colocación del artefacto en un supuesto de *skimming* o el envío de los correos electrónicos en uno de *phishing* no solo no ponen en peligro al objeto de bien jurídico tutelado por dicha norma, sino que tampoco presentan una conexión temporal con la acción típica ni su resultado. En efecto, sería incluso dudoso afirmar que el mero hecho de instalar el aparato importa una incidencia en la esfera de la víctima que, a esa altura, aún no realizó su parte. A todo evento, sea que el plan del autor fuera confeccionar tarjetas apócrifas para realizar compras o efectuar estas últimas solo mediante el uso de los datos de los plásticos bancarios, restarían aún varios actos intermedios desde la instalación del dispositivo hasta esos momentos. Es decir, estos

[76] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala VI, causa n.° 26.683, "CASTELLINI, Alfredo José y otros", 30 de marzo de 2005 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 30 de julio de 2020).

[77] Es dable aclarar que ambas modalidades son similares desde la perspectiva del comienzo de ejecución de la defraudación, pero, según el Código Penal, apoderarse de la tarjeta sería constitutivo de hurto y apoderarse de los datos no.

primeros pasos no estarían ni siquiera incluidos en la etapa inmediatamente anterior a la acción típica.

Entiendo que este razonamiento puede generar cierta confusión con el criterio defendido por el máximo tribunal, puesto que el colocar la *lectograbadora* en el cajero o enviar un correo electrónico simulando pertenecer a una institución bancaria bien podría ser considerado una conducta dirigida a la obtención de la información de las tarjetas y ello, según dicha interpretación, conforma el principio de ejecución de la defraudación cometida con tarjetas o sus datos. Sin embargo, por los motivos recién expuestos, es claro que estos primeros pasos, aunque efectivamente orientados a captar datos de manera no autorizada para defraudar, no representan el inicio de la tentativa de estos casos especiales de estafa. Al respecto, pese a que la decisión sobre el inicio de la tentativa no se debe tomar en abstracto, creo necesario hacer una aclaración de carácter general con relación al tipo penal de estafa.

Tal como se indicó anteriormente, para que se configure este delito es necesario que se presente la secuencia: engaño, error, disposición patrimonial y perjuicio -o disposición patrimonial perjudicial-. En este entendimiento, dado que, en general, es la víctima la que realiza la disposición patrimonial que la perjudica, se entiende que la estafa se trata de un supuesto de autoría mediata tipificada[78] en el que el sujeto pasivo obra como instrumento del autor. Desde este punto de vista se sostiene que, en principio y en casos normales, "existe tentativa de estafa desde el momento en que comienza la ejecución de influencia del autor sobre el sujeto pasivo"[79], esto es, a partir del despliegue de la acción engañosa. Desde otra perspectiva se considera que "en la autoría mediata el criterio que debe considerarse correcto no es la intervención del hombre de atrás sobre el instrumento, sino la puesta en marcha de la realización del tipo por parte de dicho instrumento"[80]. Es que hay casos en los que la acción engañosa solo busca generar la confianza necesaria para, luego -e incluso quizá en otro lugar-, concretar el ardid que lleva a la realización del tipo. Desde este punto de vista, "es preciso considerar si la agresión desencadenada por el autor contra el patrimonio protegido, por medio de la víctima engañada, ha alcanzado un grado de desarrollo que le haga fluir directamente hacia la realización del tipo"[81]. Sin

[78] RIGHI, *Delito de estafa*, 2017 [2015], pp. 169 y 170; JAKOBS, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación*, 1997 [1983], p. 771.
[79] RIGHI, *Delito de estafa*, 2017 [2015], p. 170.
[80] JESCHECK/WEIGEND, *Tratado de Derecho Penal. Parte General* (traducción de Miguel OLMEDO CARDENETE), 5.ª ed., Comares, Granada, 2002, p. 560.
[81] MAURACH/GÖSSEL/ZIPF, *Derecho penal. Parte general* (traducción de Jorge BOFILL GENZSCH), t. II, 7.ª ed., Astrea, Buenos Aires, 1995, p. 23.

perjuicio de esta distinción, en definitiva, la consideración de este delito como un supuesto de autoría mediata tipificada podría llevar a concluir erróneamente que, en la defraudación cometida con una tarjeta falsificada o sus datos, en tanto casos especiales de estafa, los actos dirigidos a la obtención de la información de los plásticos bancarios configuran el inicio de la tentativa.

Dicho esto, considero necesario advertir que, aunque los fraudes tipificados en el artículo 173, inciso 15, del Código Penal, son en efecto casos especiales de estafa, no necesariamente responden a su misma secuencia ni forma de intervención delictiva cuando son cometidos mediante *skimming* y/o *phishing*. Dos reflexiones al respecto.

En primer lugar, en estos supuestos no existe por regla una mente errada que, tras ser engañada, realiza una disposición patrimonial. El autor bien puede hacerse de la información de los plásticos y luego utilizarlos sin haber necesitado valerse de terceros. En particular, piénsese el caso de quien obtiene los datos de una tarjeta mediante *skimming* y luego los usa para confeccionar una tarjeta apócrifa con la que extrae dinero de un cajero automático. En similar sentido, el autor del *phishing*, tras obtener la información en cuestión, tampoco necesita siempre de la víctima ni de terceros para llevar a cabo la defraudación puesto que puede, por ejemplo, realizar una compra *online*. En todo caso, el aporte de los damnificados engañados estaría dado a la hora de la captación de sus datos, pero no necesariamente al momento de la obtención de un beneficio patrimonial. En este orden de ideas, adviértase que, en las modalidades de comisión previstas en la norma en cuestión, el fraude puede ser realizado por medio de una operación automática, esto es, sin intervención de personas que obren como instrumentos del sujeto activo al realizar la disposición patrimonial lesiva. Así las cosas, se trataría en general de casos de autoría directa y no mediata, con las consecuencias que ello pueda tener en el posterior tratamiento de su principio de ejecución.

En segundo lugar, pese a que estos supuestos pueden configurarse sin la necesidad de una mente errada que realice la disposición patrimonial perjudicial, puede ocurrir que sí se presente dicha secuencia. Así, en algunos casos "las hipótesis mencionadas por el tipo del inc. 15 pueden implicar, efectivamente, que se induzca a error (v.gr., el uso de una tarjeta falsificada ante un comerciante)"[82]. Pero aun en ese supuesto, es este último ardid y no aquel empleado para la obtención de los datos el que resulta típico de este delito. Es que, en definitiva, el engaño para captar los datos no es prototípico de esta

[82] GOTTHEIL/LÓPEZ, *Revista de Derecho Penal y Procesal Penal*, 2004, p. 733.

defraudación; sí lo es aquel que se encuentra en relación directa con la disposición patrimonial. Este último forma parte de la influencia que el autor ejerce sobre el instrumento -tercero distinto a la víctima-, tras la cual el hecho debería fluir hacia la consumación sin su intervención.

Ahora bien, descartado que la acción de colocar el *skimmer* o enviar un correo electrónico engañoso configure el inicio de la tentativa de los supuestos de fraude tipificados en el artículo 173, inciso 15, del digesto sustantivo, corresponde determinar qué calificación legal cabe asignar a los actos en cuestión. En el primer caso, el acto de instalar el dispositivo en la ranura del cajero automático sería constitutivo del delito de tenencia de un instrumento conocidamente destinado a cometer una falsificación, en los términos del artículo 299 de dicho ordenamiento. A lo sumo, la discusión podría estar en definir si, además, esta acción significa el principio de ejecución de la posterior falsedad -en caso de que el autor pretenda confeccionar una tarjeta apócrifa con los datos obtenidos-. Sin embargo, al menos en este estadio del desarrollo del plan delictivo, la falsificación (art. 282, en función del art. 285, del Código Penal) no se encuentra iniciada. En primer lugar, si el legislador previó que el acto de conservar dicho artefacto sea merecedor de una pena, entonces significa que esa conducta no es aún una tentativa de falsificación. En segundo término, el hecho de que la colocación del dispositivo parezca excederse de una mera tenencia no debe llevar a la conclusión de que, entonces, el comportamiento importa el comienzo de la falsificación. Con todo, no concurren en dicha conducta los conceptos de conexión temporal estricta e incidencia en la esfera del tipo que, como se explicó, exige buena parte de la doctrina para determinar si ciertos actos forman parte de la etapa estrictamente anterior a la acción típica, que es abarcada por la tentativa. Al respecto, se ha dicho que "la falsificación de moneda mediante imitación (§ 146 I núm. 1) comienza al ponerse a realizar el acto de falsificación: por ejemplo, al disponer de los objetos mencionados en el § 149 [preparación de la falsificación de moneda y de sellos], con el fin de ponerse al trabajo sin demora para realizar la falsificación"[83].

En el segundo caso, es decir, aquel en el cual el autor envía correos electrónicos engañosos a distintos destinatarios para lograr que estos aporten los datos de sus tarjetas bancarias, la conducta no configura delito alguno. En este supuesto, el individuo se vale de algún aparato tecnológico -v.gr., su computadora personal- para enviar un *email* y no

[83] ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 481.

de un instrumento cuya tenencia resulta *per se* ilegal. Por ello, de aceptarse la tesis de que tal comportamiento no forma parte de la tentativa de defraudación, entonces debe concluirse que la acción es atípica.

2. El autor obtiene los datos de las tarjetas bancarias

Dentro de este grupo de casos es posible incluir supuestos en los que, por ejemplo, el autor ya retiró la *lectograbadora* del cajero automático con los datos de distintas tarjetas bancarias o recibió la información solicitada vía correo electrónico. Asimismo, se podría pensar en el accionar del empleado de un comercio que, al tener en su poder la tarjeta de pago del cliente, la introduce por su dispositivo dado que, aunque recurriendo a una metodología distinta, también logra hacerse de sus datos. En definitiva, se trata de casos en los que el autor ya tiene en su poder la información de las tarjetas con la que piensa cometer un fraude. Luego, las circunstancias de unos y otros supuestos serán determinantes a la hora de decidir qué calificación legal corresponde adoptar.

En un caso de *skimming* ya citado (ver nota al pie n.° 72), en el que no se habían corroborado aún perjuicios patrimoniales y no se podía establecer qué información almacenaba el dispositivo incautado a los imputados, la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal sostuvo que los sobreseimientos dictados en primera instancia eran prematuros pues no se podía descartar que la acción hubiera trascendido la etapa preparatoria y conformado el principio de ejecución de la maniobra defraudatoria. A ese efecto, los jueces intervinientes consideraron que se debía establecer si medió en los hechos una "factibilidad de afectación patrimonial en concreto"[84]. Sobre el fallo se ha dicho que "[p]arece evidente que en las concretas circunstancias del caso, el comportamiento supuso un evidente peligro de menoscabo del bien jurídico, o si se prefiere, una conducta que actuó sobre el objeto de tutela llegando inclusive a vulnerar la esfera de protección de la víctima, por lo que lo adecuado a derecho era considerar que hubo comienzo de ejecución, y por lo mismo, una tentativa punible (arts. 42 y 173, inc. 15, CP)"[85]. Sin embargo, pese a que la obtención de datos puede significar una intromisión en la esfera de la víctima, entiendo que la ausencia de la conexión temporal entre esa conducta y la acción típica impediría

[84] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.663, "OLIVEIRA RIVAS, Fabio y otros s/ defraudación", 20 de agosto de 2008 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).
[85] RIGHI, *Delito de estafa*, 2017 [2015], p. 279.

concluir que existió una tentativa de defraudación. Tanto es así que los jueces, aunque revocaron la resolución de primera instancia por considerarla prematura y advirtieron que las maniobras podían haber trascendido la etapa preparatoria, no afirmaron de manera terminante que estas hayan configurado un principio de ejecución. En rigor, ello era lo que entendieron que aún se debía constatar.

Ahora bien, si los casos del apartado anterior ya podían ser considerados actos dirigidos a la obtención de datos y, entonces -según el criterio de la Corte-, parte del principio de ejecución de la defraudación, los mencionados en el presente título deberían con toda seguridad encontrarse también alcanzados por dicho razonamiento. En este sentido, nótese que se trata de acciones por las que no solo se pretende captar la información que luego se utilizará para cometer un fraude, sino de conductas por las que se concreta efectivamente dicho fin. Sin embargo, como he sostenido, es incorrecto aplicar sin más el criterio del máximo tribunal en estos casos.

Adviértase que, aunque las conductas bajo análisis se encuentren efectivamente orientadas a la captación de la información con la que luego se buscará cometer un fraude, en principio no parecen formar parte de la etapa estrictamente anterior a la acción típica que quedaría abarcada por la tentativa. Es que, como se sostuvo, el engaño vinculado a la obtención de datos no es prototípico de este caso especial de estafa, mientras que sí lo es aquel que da lugar al acto de disposición patrimonial perjudicial. Permítaseme ejemplificar esta cuestión con un supuesto más tradicional. Un individuo engaña a otro y logra que, por error, le entregue el *ticket* necesario para retirar su automóvil del garaje en el que se encuentra estacionado. Una hora después, simula ser el dueño del vehículo ante el cuidador del lugar -para lo cual presenta el comprobante previamente obtenido- y logra que este último le entregue, por error, el auto. En el caso, solo este segundo engaño -y no aquel mediante el cual se obtuvo el *ticket*- es típico del delito de estafa dado que se encuentra en relación directa con la disposición patrimonial perjudicial. De hecho, en el primer tramo puede ni siquiera existir un ardid: el autor hurta la billetera de la víctima en la que se encuentra contenido el *ticket* y luego logra que el encargado del garaje le dé el vehículo contra la entrega de dicho comprobante. Allí, queda más claro aún que el primer momento -en el que casualmente puede existir un engaño- no forma parte de la estafa que se materializa después con el ardid que da lugar a la disposición patrimonial perjudicial.

Si en contra de lo que aquí argumento se considerara que el engaño de la captación no autorizada de datos de tarjetas constituye un elemento del tipo en cuestión, su realización no debe llevar a la errónea conclusión de que, entonces, se trata de un acto de

tentativa. En este sentido, "[d]ado que el autor tiene que ponerse inmediatamente a realizar la conducta *en conjunto* típica, el realizar una parte de la acción típica sólo fundamenta una tentativa si en ello hay, a la vez, un ponerse inmediatamente a realizar los otros **actos parciales** necesarios para realizar el tipo"[86]. Resulta indudable que, en los casos bajo análisis, no se presenta esa conducta en conjunto típica. En resumen, la maniobra engañosa empleada para captar información (sea por medio de *phishing* o *skimming*) es preparatoria y no ejecutiva de la defraudación.

En el caso en el que el autor pretende cometer el fraude con una tarjeta falsificada, cuando logra hacerse de dicha información, aún debe llevar a cabo la falsedad que lo separa -temporalmente hablando- de la acción que puede provocar perjuicios a patrimonios de terceros. Tal vez se pueda predicar que la obtención no autorizada de datos implique por sí sola una intromisión en la esfera de la víctima pero, como se dijo, el autor todavía tendría que realizar varios actos antes del que ya resulta típico de la defraudación. De este modo, además, la incidencia en la esfera de la víctima no concurriría conjuntamente con la exigida conexión temporal estricta que debe existir entre el acto en cuestión y la acción típica.

Si el plan del autor fuera, tras captar los datos, efectuar inmediatamente una compra *online* con ellos -por ejemplo, en un supuesto de *phishing* en el que el sujeto logró pescar la información-, esta conclusión sería más discutible. En ese último bloque de actos sí concurrirían conjuntamente los conceptos auxiliares de conexión temporal estricta e incidencia en la esfera de la víctima. Entonces, sería imaginable -aunque solo en supuestos muy particulares- una tentativa. A todo evento, si en ese caso puntual se aceptara que existió principio de ejecución -lo que, como dije, es discutible-, ello no se debería a la pesca de información en sí sino a que esta, en ese supuesto, fue realizada estrictamente antes de la acción típica. En cambio, en cualquier otro hecho de *phishing* en el que la intención del pescador no es concretar el fraude al instante de haber obtenido la información, sino quizá en otro momento posterior, se debería sostener que la defraudación no fue iniciada.

Según este razonamiento, en términos generales, se debería concluir que la captación no autorizada de datos de tarjetas forma parte de la preparación de la posterior defraudación cometida con ellos. En definitiva, en los dos medios de comisión previstos en el artículo 173, inciso 15, del Código Penal, que aquí se analizan (tarjeta falsificada y

[86] FRISTER, *Derecho Penal. Parte General*, 2016 [2006], p. 486.

uso de sus datos), la acción típica comenzaría cuando el autor se dispone a utilizarlos con el fin de obtener un beneficio patrimonial.

¿Podrían ser las conductas en cuestión consideradas ejecutivas de la falsificación si el autor pensara confeccionar tarjetas apócrifas para cometer el fraude? Ello sin duda dependerá de las particulares circunstancias del hecho. La cuestión fue también analizada en el fallo citado hace algunos instantes. En dicha oportunidad se incautaron, además del mencionado dispositivo, un papel con inscripciones de números de tarjetas y tarjetas sin información en sus bandas magnéticas -es decir, vírgenes-. Frente a ese panorama probatorio, se sostuvo que el proceso de falsificación no comienza con la toma de datos sino cuando estos "comienzan a volcarse en un plástico nuevo al que, además se le da la apariencia externa de una tarjeta legítima. En ese sentido, la conducta de quien se encuentra copiando bandas magnéticas por medio de estos dispositivos técnicos resultaría atípica en relación con la figura contemplada por el artículo 285 del C.P., en función del art. 282, sin perjuicio de que, si hay luego comienzo de ejecución, esas conductas pueden ser punibles como participación en el hecho típico"[87]. Aunque la solución puede haber sido atinada para ese caso puntual -puesto que, como sostuve (página 34), la acción dirigida a obtener la información no constituye *per se* el inicio de la falsificación-, a diferencia de dichos jueces, interpreto que el principio de ejecución de la falsedad no debe ubicarse en el momento en el que los datos se vuelcan efectivamente en la tarjeta sino en los actos estrictamente anteriores como, por ejemplo, cuando el autor ya cuenta con los elementos necesarios (plásticos con las bandas magnéticas vacías, datos captados, etcétera) y se encuentra dispuesto a emplearlos. No hay duda de que volcar la información en la tarjeta vacía constituye la conducta de falsificar -prohibida según el artículo 282, en función del 285, del código de fondo- pero la tentativa alcanza también la zona estrictamente previa a la acción típica.

En resumen y por los motivos expuestos, las conductas analizadas no serían constitutivas de la tentativa de defraudación. Si en el supuesto puntual de *phishing* mencionado se aceptara que existió principio de ejecución -lo que, como sostuve, no es del todo evidente-, ello no se debería a que la pesca de información es en sí misma un acto ejecutivo por naturaleza sino a que, en ese caso, fue realizada estrictamente antes de la acción típica. Quien ya retiró del cajero el dispositivo con la información registrada,

[87] CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CAPITAL FEDERAL, Sala IV, causa n.° 34.663, "OLIVEIRA RIVAS, Fabio y otros s/ defraudación", 20 de agosto de 2008 (http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm, consultado el 5 de noviembre de 2020).

pasó la tarjeta de pago del cliente por dicho artefacto o recibió los datos vía correo electrónico, no ha comenzado aún a cometer una defraudación. Por lo demás, si el objetivo de las maniobras dirigidas a obtener la información fuera luego confeccionar tarjetas falsas, estas tampoco deben ser consideradas actos ejecutivos de la falsificación en la medida en la que el autor aún debe realizar otras acciones para, en otro momento y lugar, con todos los materiales necesarios, volcar los datos en los nuevos plásticos. En función de lo expuesto, si el autor realiza exitosamente el *phishing* (esto es, lanza los *emails* y recibe los datos bancarios solicitados), pero no tiene ningún elemento de falsificación, su conducta no constituye delito alguno (ni tenencia de instrumentos destinados a falsificar, ni falsificación, ni defraudación).

3. Posibles acciones que suceden a la captación de datos

En este último grupo de casos se estudiarán distintos actos que pueden ocurrir después de la obtención no autorizada de datos de tarjetas bancarias. En primer lugar y al efecto de completar el análisis entre los delitos de falsificación y defraudación cometida mediante tarjeta falsificada, se tratará el supuesto en el que el autor ya confeccionó un plástico apócrifo con la información pescada. En segundo lugar, a modo de introducir la cuestión -¿problemática?- de la venta de datos bancarios -u otros-, se examinará el caso de quien, habiendo obtenido exitosamente la información de diversas tarjetas con la intención de cometer un fraude, cambia de plan y, en cambio, la vende a terceros.

Como se sostuvo, el comienzo de ejecución del delito de falsificación de tarjetas de compra, crédito o débito (art. 282, en función del 285, del Código Penal) puede ubicarse en el momento en el que el autor ya cuenta con los materiales necesarios para llevar a cabo la falsedad y se dispone a utilizarlos; es decir, la etapa inmediatamente anterior a que, por ejemplo, empiece a volcar los datos en los plásticos. De este modo, es posible afirmar que en ese instante no solo no existe la posibilidad de interponer otro acto -esencial- antes de la realización típica, sino que, además, concurren de manera conjunta los ya mencionados requisitos de conexión temporal estricta e incidencia en la esfera del tipo[88].

Ahora bien, desde la perspectiva de la materia de prohibición de la defraudación cometida mediante una tarjeta falsificada (art. 173, inciso 15, del ordenamiento

[88] Recuérdese que, en los casos en los que falta una esfera especial en el lado del atacado -como en la falsificación de moneda-, se debe tomar como punto de referencia la esfera del tipo. Al respecto, ver ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 481.

sustantivo), el hecho de que el autor haya comenzado -o incluso concretado- la falsedad no quiere decir que, entonces, haya iniciado también el fraude. Para ello es necesario que, según su plan, se disponga a emplear la tarjeta apócrifa con ese fin -por ejemplo, usarla para realizar una compra-. En este sentido, quien ha obtenido los datos mediante *skimming* y luego confeccionado un plástico falso con los mismos, no ha empezado a cometer una defraudación si aún no se dispone a utilizarlo. A todo evento, esa falsificación, punible como un delito autónomo, forma parte de la preparación de la posterior defraudación y podría eventualmente concurrir con esta última si el autor la llevara a cabo. En definitiva, en estos supuestos la tentativa del fraude comenzaría, por ejemplo, cuando el autor pretende hacer incurrir en un error al comerciante ante quien exhibe la tarjeta apócrifa o intenta extraer dinero de un cajero automático con ella[89].

Por último, me detendré en el caso hipotético en el cual el autor, tras obtener los datos de las tarjetas bancarias, abandona su primigenio plan fraudulento -que podía ser, por ejemplo, realizar con ellos compras por Internet- y, en cambio, los vende a un tercero. Así, obtiene un beneficio económico por esa venta y no a raíz de una disposición patrimonial que perjudica a la víctima. No conoce personalmente al comprador ni tampoco sabe qué uso dará a los datos en cuestión[90]. Al efecto de su estudio, podemos dividir el hecho en dos momentos: en el primero tiene lugar la captación de información y en el segundo, la venta.

Una buena parte del análisis vinculado a si el *skimming* y el *phishing* configuran o no el principio de ejecución de la defraudación cometida con tarjetas falsificadas o el uso no autorizado de sus datos ya fue realizada. Por los motivos expuestos anteriormente, esos actos de obtención de datos deben ser considerados preparatorios y no ejecutivos de los casos especiales de estafa tipificados en el artículo 173, inciso 15, del Código Penal. Según este razonamiento, entonces, quien ha captado la información por medio de un *skimmer* podría ser considerado responsable por la tenencia de un instrumento conocidamente destinado a falsificar (art. 299 de dicho ordenamiento) pero no por haber empezado a defraudar ni a falsificar. A su vez, quien lo hizo por medio de una maniobra

[89] Es claro que se deberá determinar si, para la tentativa, basta con que el autor merodee por un comercio con la tarjeta apócrifa o si, además, debe habérsela entregado al empleado del local a quien pretende hacer incurrir en un error. Pero lo que es seguro es que la confección de dicho plástico falso no es el principio de ejecución del fraude.

[90] Al respecto, téngase presente que el intercambio de datos, información, etcétera, podría darse de manera anónima -tanto para quien publica contenido como para quien lo consume- en mercados negros digitales. Sobre el funcionamiento de estos últimos y su relación con la *Deep and Dark Web* y los navegadores que permiten el anonimato -v.gr., TOR-, ver SALLIS, "Desafíos de la investigación de los delitos informáticos en la '*Deep & Dark Web*'", en DUPUY/KIEFER, *Cibercrimen*, t. I, 2020, pp. 601 a 616.

de *phishing* no habría realizado una conducta penalmente relevante. Por lo tanto, en el caso hipotético presentado, el autor que tras captar los datos de las tarjetas desiste[91] de su plan inicial, no ha ejecutado de momento una acción típica (a lo sumo, como se dijo, su conducta se podrá encuadrar en las previsiones del mencionado artículo 299, si contó con una *lectograbadora*).

En resumen, la obtención no autorizada de información de tarjetas bancarias es parte de la etapa preparatoria y no ejecutiva de la defraudación cometida con ella. La pregunta que resta responder, entonces, es qué adecuación legal se debe dar a la posterior venta de los datos captados. A tal fin, es necesario reflexionar sobre dos interrogantes. Primero, ¿prohíbe el Código Penal dicho comportamiento? Segundo, quien vende la información, ¿tiene alguna intervención en el delito que con ella luego comete quien la compra? De esto dependerá la solución del caso, es decir, cómo se debe resolver el supuesto en el que el autor, tras obtener los datos de distintas tarjetas bancarias, decide no concretar el fraude y, en cambio, vender dicha información a terceros.

En primer lugar, el Código Penal no prevé sanciones para la venta de datos personales[92] como pueden ser los de tarjetas bancarias. La protección que el legislador ha dado a la información personal en el digesto sustantivo se limita a la prohibición de acceder de forma no autorizada a un banco de datos personales, de proporcionar o revelar a otro información allí registrada y de insertar o hacer insertar ilegítimamente datos en un archivo de datos personales (art. 157 bis del Código Penal). Al respecto, se ha dicho que "la ley argentina no siguió un camino tan amplio, pues el art. 157 bis, Cód. Penal, no penaliza la venta de datos personales en forma ilegal, aunque esto sí puede constituir un ilícito civil y administrativo (art. 11, ley 25.326 y Disposiciones de la Dirección Nacional de Datos Personales). El problema de la venta de datos, que es el talón de Aquiles de la ley 25.326, se podría decir que no tiene solución, por ahora"[93]. En estos términos, es

[91] Desistir en el sentido literal de dejar de hacer algo que se había proyectado o empezado a realizar y no en el significado jurídico de la norma del art. 43 del Código Penal que, por cierto, está dirigida al autor de tentativa -que, como se explicó, no es el del caso hipotético planteado-.

[92] La Ley de Protección de Datos Personales los define -de manera muy amplia- como: "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" (art. 2, Ley 25.326). De esta forma, es posible incluir en esa información a la referida a las tarjetas bancarias de una persona.

[93] PALAZZI, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 2016 [2009], p. 130. Al respecto, considero prudente advertir que en la afirmación aquí citada -que forma parte del desarrollo que PALAZZI realiza sobre los delitos relacionados con la protección de datos personales- el autor no se refiere puntualmente a datos de tarjetas bancarias sino al concepto amplio de datos personales definido en la Ley 25.326. A su vez, es dable remarcar que la posibilidad de que la venta de datos constituya un ilícito civil y administrativo, al menos a mi entender, se encuentra limitada a los sujetos que intervienen en el tratamiento

posible afirmar que el autor del supuesto hipotético aquí analizado no comete una conducta típica al vender la información previamente obtenida.

En segundo lugar, corresponde determinar si dicho comportamiento constituye alguna clase de intervención punible en el delito que con los datos en cuestión comete quien los adquiere. Por ejemplo, piénsese que este último luego los usa para realizar una compra telefónica u *online* y, de este modo, lleva a cabo una defraudación en los términos del artículo 173, inciso 15, segundo supuesto, del Código Penal. Tal como se explicó, con excepción de las previsiones del artículo 299 de dicho ordenamiento, el autor del caso no realiza una acción típica al obtener la información de las tarjetas bancarias ni al venderla a un tercero, puesto que la primera conducta no configura *per se* una tentativa de defraudación ni de falsificación y la segunda no está prevista en nuestro código de fondo. Entonces, de existir una respuesta punitiva para el caso, esta se vería limitada a una eventual participación en la defraudación que comete otro. Sin embargo, la posibilidad de una intervención de este tipo, al menos en las circunstancias descriptas, no sería del todo evidente. En este sentido recuérdese que, en el supuesto planteado, quien pesca y luego vende los datos no conoce el destino que se les dará. En función de ello, dado que "la participación es típica sólo cuando es dolosa…"[94], se podría llegar a concluir que esa persona que captó y vendió la información que luego fue utilizada para defraudar no realizó una conducta penalmente relevante.

En este orden de ideas, la punibilidad de la intervención del vendedor de datos en la defraudación cometida por quien se los compra deberá definirse según elementos de la faz subjetiva, es decir, dependerá del conocimiento que este tenga del plan fraudulento de su comprador. En el caso recién descripto, ante el absoluto desconocimiento del proyecto delictivo posterior -y, por ende, ante la posible ausencia de dolo-, se sostuvo que la conducta en cuestión podría ser atípica. Claro está, distinta sería la solución si se tratara de un acuerdo conjunto entre quien pesca los datos y quien concreta el fraude cometido con ellos. En ese supuesto, sí sería posible una participación -en el caso, necesaria (art. 45, C.P.)- de quien obtuvo la información de las tarjetas bancarias. Sin embargo, dada la

de dichos datos y que, por ello, tienen un deber de confidencialidad sobre los mismos, pero no a la generalidad de las personas (arts. 10 y 11, Ley 25.326).

[94] D'ALESSIO (Dir.)/DIVITO (Coord.), *Código Penal de la Nación comentado y anotado*, t. I, 2011 [2005], p. 783. En este sentido -es decir, el de definir como dolosa la colaboración típica del partícipe-, ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 204 y, en nuestro país, ZAFFARONI/ALAGIA/SLOKAR, *Manual de Derecho Penal: Parte General*, 2014 [2005], p. 624, entre otros. Tal como se advierte en la obra de D'ALESSIO (Dir.)/DIVITO (Coord.) aquí citada, "[s]i bien algunos autores admiten la participación culposa, por lo general no se acepta la participación culposa en un hecho doloso, ni la participación dolosa o culposa en un hecho culposo" (ver p. 783 y, particularmente, sus notas al pie n.° 325 a 329).

naturaleza accesoria de la participación, el aporte solo tomaría relevancia jurídico-penal cuando el autor del hecho principal comienza su ejecución. Si se aceptara -como hace parte de la doctrina[95]- una atribución de responsabilidad a título de coautor al que interviene en la etapa preparatoria del delito -como es la obtención de datos de tarjetas en la defraudación cometida con ellos-, el pescador podría ser considerado coautor del fraude. Pero tanto en el supuesto hipotético analizado anteriormente como en cualquier otro en el que quien capta la información luego se la vende a un tercero en desconocimiento del uso que este último le dará, la tipicidad de la intervención no parecería admisible. En los casos de venta de datos de plásticos bancarios en mercados negros digitales, el pescador puede sospechar que quien adquiere la información por esa vía tiene un fin delictivo, pero no sabe si este efectivamente cometerá un delito, ni cuál será (estafa, extorsión…), ni cuándo, cómo o dónde lo llevará a cabo si es que lo hace, etcétera. En estos términos, no parecería posible una imputación por esa venta puesto que esta no lo convierte en partícipe de cualquier delito que el comprador vaya a cometer en el futuro con la información.

En definitiva, la pesca y venta de datos no estaría prohibida. De hecho, en razón de lo expuesto, se debería también concluir que quien compra la información tampoco realiza una acción típica por su mera adquisición -cualquier hipótesis de encubrimiento debería descartarse en función de la inexistencia de un delito precedente- en la medida en la que no lleve a cabo otro delito.

En conclusión, la persona que obtiene mediante *skimming* datos de tarjetas bancarias que luego vende a terceros, no realiza una conducta típica más allá de la descripta en el artículo 299 del código de fondo, y la que lo hace por medio de maniobras de *phishing*, no realiza acción típica alguna. Dichas acciones solo podrían ingresar al ámbito de lo prohibido como una colaboración al injusto de otro -por ejemplo, el comprador- si este comenzara la ejecución y si se pudiera probar la existencia del dolo (como dije, no siempre será del todo evidente). Esta conclusión, aquí analizada para un hecho en el que el autor pretendía inicialmente cometer una defraudación, resulta también aplicable a supuestos en los cuales los pescadores de información se dedican exclusivamente a obtener y vender datos de tarjetas bancarias -u otros datos personales-

[95] JAKOBS, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación*, 1997 [1983], pp. 749 y 750.

en vez de a estafar[96]. Ello porque dichas conductas -con excepción de la mera tenencia de un instrumento destinado a falsificar en el caso del *skimming*- no se encuentran tipificadas como delitos autónomos, no son ejecutivas del fraude ni podrían ser siempre consideradas un aporte doloso al hecho delictivo principal de otro si no se tuviera conocimiento real del mismo. De este modo, si tres o más personas se organizaran para obtener y luego vender datos de tarjetas bancarias, ni siquiera se configuraría una asociación ilícita en los términos del artículo 210 del Código Penal, en tanto la norma exige que dicha banda se encuentre destinada a cometer delitos. Por lo demás, la adquisición de datos personales tampoco sería típica en la medida en la que no se lleve a cabo otro delito.

B. Síntesis del análisis

A partir del estudio de casos realizado en los apartados precedentes y por una cuestión de claridad expositiva -o al menos un intento de ello-, apuntaré a continuación algunas conclusiones que entiendo permitirán resumir y ordenar los principales argumentos hasta aquí desarrollados:

- Las defraudaciones previstas en el artículo 173, inciso 15, del Código Penal, cuando son cometidas mediante *skimming* o *phishing*, no necesariamente responden a la secuencia tradicional de la estafa ni a su forma de intervención delictiva. Por medio de un engaño el autor obtiene los datos de las tarjetas bancarias y, luego, puede materializar por sí o por terceros (caso en el cual desplegará otro ardid) la disposición patrimonial lesiva.

- El engaño empleado para la obtención de datos no es prototípico de esta defraudación, sí lo es aquel que se encuentra en relación directa con la disposición patrimonial perjudicial. Este último forma parte de la influencia que el autor ejerce sobre el instrumento -tercero distinto a la víctima-, tras la cual el hecho debería fluir hacia la consumación sin su intervención. De concretar el sujeto activo el fraude sin valerse de otros -v.gr., por medio de una operación automática-, el comienzo de ejecución también debe ubicarse en los últimos actos que realiza y luego de los cuales debería materializarse

[96] Así como el *phishing* es utilizado con fines fraudulentos, también lo es con la sola intención de vender los datos pescados. Al respecto, se ha señalado que "normalmente el *phisher* no explota por sí mismo la información obtenida, sino que la vende a terceros" (MIRÓ LLINARES/GÓMEZ BELLVÍS, "La estafa informática: fenomenología y respuesta jurídica", en DUPUY/KIEFER, *Cibercrimen*, t. II, BdeF, Montevideo-Buenos Aires, 2020, p. 19 y sus citas -adviértase que en la nota al pie n.° 40 se hace referencia específicamente a la venta de números de tarjetas de crédito en el mercado negro-).

la disposición patrimonial, pero no cuando obtiene los datos que luego utilizará para defraudar.

- En definitiva, las maniobras de *skimming* o *phishing*, como modalidades de obtención no autorizada de datos, no son el comienzo de la tentativa de las defraudaciones del artículo 173, inciso 15, del Código Penal, sino meros actos preparatorios.

- Dichas conductas tampoco son el principio de ejecución de la falsificación de tarjetas prevista en el artículo 282, en función del 285, del ordenamiento sustantivo. Esta última comienza en el momento en el que el autor ya cuenta con los elementos necesarios (plásticos con las bandas magnéticas vacías, datos captados, etcétera) y se dispone a emplearlos. En ese instante, a diferencia de aquel en el que se capta la información, no solo no existe la posibilidad de interponer otro acto -esencial- antes de la realización típica sino que, además, concurren de manera conjunta los requisitos de conexión temporal estricta e incidencia en la esfera del tipo. Entonces, esta es la etapa inmediatamente anterior a la ejecución del verbo -"falsificare"- descripto en el tipo y, por ende, aquella que queda abarcada por la tentativa. Con todo, el que el autor haya comenzado -o incluso consumado- la falsedad no quiere decir que, entonces, haya iniciado también el fraude.

- En función de lo expuesto (es decir, que las maniobras de obtención no autorizada de datos en cuestión no son el comienzo de la tentativa de defraudación ni de falsificación), el *skimming* queda solo alcanzado por las previsiones del artículo 299 del digesto sustantivo y el *phishing* es atípico. Esta última modalidad de captación de datos no se encuentra tipificada de manera autónoma[97]. De este modo, quien únicamente capta información de tarjetas bancarias -u otros datos personales- por medio de esta vía, no realiza de momento una conducta penalmente relevante según la legislación vigente.

- A su vez, dado que el Código Penal tampoco prevé sanciones para la venta de datos personales -como pueden ser los de tarjetas bancarias-, quien obtiene dicha información de forma no autorizada y luego la vende, no comete delito alguno. A lo sumo, la punibilidad de esa última conducta queda limitada a una colaboración en el hecho

[97] En este sentido, CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "A diez años de la ley de delitos informáticos. Balances y propuestas", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 1, 2019, p. 146; CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, 2019, pp. 118 y 120; TEMPERINI/MACEDO, "Aspectos legales de la ingeniería social: análisis sobre la responsabilidad civil y penal del ingeniero social", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 3, Hammurabi, Buenos Aires, 2020, pp. 82 y 83; DE LUCA, "Delitos informáticos, apuntes de 2016", en DUPUY/KIEFER, *Cibercrimen*, t. I, 2020, p. 16; GARAT/REALE, "La reforma penal en materia de cibercrimen en la República Argentina", en DUPUY/KIEFER, *Cibercrimen*, t. II, 2020, pp. 520 y 521; entre otros.

principal -v.gr., estafa, extorsión, etcétera- de otro. Sin embargo, el desconocimiento sobre los elementos del proyecto delictivo posterior podría llegar a excluir la tipicidad del aporte en algunos casos y, a todo evento, las acciones bajo análisis solo tomarían relevancia jurídico-penal si el autor del injusto principal comenzara su ejecución. Asimismo, el hecho de que la obtención y la venta de datos resulten atípicas, en tanto impone descartar un delito precedente, lleva a la conclusión de que también lo será su adquisición.

- Sobre la base de estas consideraciones, tampoco cabría una imputación en los términos del artículo 210 del digesto sustantivo contra quienes tomaran parte en una banda de tres o más personas destinada a obtener y vender datos personales, en tanto la norma exige que dicha asociación se encuentre destinada a cometer delitos.

V. La obtención ilícita de datos personales como delito autónomo

Hasta aquí he analizado si la obtención ilegítima de datos de tarjetas bancarias es o no el principio de ejecución de las defraudaciones cometidas con tarjetas falsificadas o el uso no autorizado de sus datos. A partir de ello, he procurado argumentar que las maniobras de captación de información -como el *skimming* y el *phishing*- son actos preparatorios y, por ende, no revisten el carácter de ejecutivos de esos casos especiales de estafa ni de la falsificación de tarjetas prevista en el artículo 282, en función del 285, del Código Penal. El desarrollo del tema, a su vez, ha dejado en evidencia que la respuesta que el código de fondo prevé para dichas conductas es prácticamente nula. En este sentido, los supuestos de *skimming* solo podrían ser encuadrados en el tipo del artículo 299 de dicho ordenamiento, mientras que el *phishing* sería atípico. Ello porque esta técnica de ingeniería social se sanciona únicamente y por vía indirecta mediante las figuras del artículo 173 ya mencionadas, pero, como se argumentó, no forma parte de la tentativa de las mismas. Entonces, en la medida en la que el pescador de datos se limite a, valga la redundancia, pescarlos, no realiza una conducta penalmente relevante.

En estos términos, dejando atrás el primer y principal interrogante sobre el que giró este trabajo, corresponde preguntarnos si la obtención ilegítima de datos financieros personales -u otros- debería tipificarse de manera autónoma, adelantando la penalidad. Según interpreto, la respuesta a esta cuestión debería apoyarse en dos puntos (uno de los cuales se abordó en estas páginas). Por un lado, la creación de un tipo de adelantamiento dependería de que la acción a tipificar no forme parte de la tentativa de otra que ya se encuentra prevista en el Código Penal. En este sentido, he argumentado que las conductas

bajo análisis son actos preparatorios desde la perspectiva de la defraudación y que no deben ser consideradas como el comienzo de una falsificación en los términos del artículo 282, en función del 285, de dicho ordenamiento. Por otro lado, deberían existir motivos que justifiquen la creación de un nuevo tipo penal para ese comportamiento en particular. Al respecto, pese a que esta cuestión merecería un examen de igual o mayor profundidad que el hasta aquí realizado y ello excedería el límite de extensión de este trabajo, intentaré aportar algunas razones a favor de que la obtención no autorizada de los datos en cuestión sea sancionada de manera autónoma.

Ya en el año 2002, en oportunidad de tratarse los proyectos que devendrían en la Ley 25.930, se advirtió que "no son tampoco típicas según la legislación penal vigente las conductas de vender, comprar, recibir, obtener o emplear ilegítimamente datos de tarjetas de crédito o débito…"[98]. Entonces, se propuso agregar como artículo 157 ter del Código Penal la sanción a quien "a) [g]rabare, reprodujere, suministrare, recibiere, traficare, almacenare o usare información o datos codificados registrados en la cinta magnética de una tarjeta de crédito o débito; b) [o]btuviere, suministrare, recibiere, traficare o usare el número de una tarjeta de crédito o débito o el número de seguridad de una de tales tarjetas o el código secreto de identificación personal de su legítimo usuario"[99]. En el año 2004, a partir de la sanción de la mencionada ley -que no incluyó la propuesta citada-, se señaló en doctrina que la misma "tampoco tipificó como delito autónomo la actividad de quien copia los datos de las tarjetas mediante el proceso conocido como *skimming*, quedando, en principio, como un mero acto preparatorio, salvo que acceda como participación de un delito posterior de falsificación (art. 282 CPen., en función del nuevo art. 285), o de la defraudación del nuevo inc. 15"[100]. Así, se sostuvo que "[s]ería esperable que en futuras reformas se legisle específicamente sobre estas conductas"[101].

Años después se pretendió agregar el *phishing* al código de fondo, pero "si bien el legislador lo incorporó como una figura patrimonial abusiva realizada por medios informáticos (art. 173, inc. 16) […] no contempló sin embargo el momento previo de 'pesca o robo de credenciales' por cuanto ello significaba atrapar conductas previas al

[98] Proyecto de ley de las diputadas GARRÉ y FALBO (2.954-D.-2001), Diario de sesiones de la Cámara de Diputados de la Nación, 26.ª reunión - 14.ª sesión ordinaria, 18 de septiembre de 2002, p. 3112.
[99] Proyecto de ley de las diputadas GARRÉ y FALBO (2.954-D.-2001), Diario de sesiones de la Cámara de Diputados de la Nación, 26.ª reunión - 14.ª sesión ordinaria, 18 de septiembre de 2002, p. 3115.
[100] GOTTHEIL/LÓPEZ, *Revista de Derecho Penal y Procesal Penal*, 2004, p. 734.
[101] GOTTHEIL/LÓPEZ, *Revista de Derecho Penal y Procesal Penal*, 2004, p. 734.

comienzo de ejecución de la maniobra de estafa propiamente dicha"[102]. Entonces, la modalidad de captación de datos en cuestión quedó sancionada única e indirectamente a través de estos casos especiales de estafa[103].

Frente a ello, en el año 2011 se propuso la incorporación al Código Penal -como artículo 157 ter, inc. 1- de la sanción para el que "[m]ediante cualquier forma de ardid o engaño, indebidamente obtuviere o captare datos personales, financieros o confidenciales…"[104]. Luego, en 2012 se propugnó agregar -como artículo 138 bis- la penalización para "el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de Internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficios para sí o para terceros"[105]. Ninguna de estas propuestas tuvo el resultado esperado. Por su parte, el Anteproyecto de Código Penal de la Nación elaborado por la comisión creada mediante el Decreto 678/2012 preveía una sanción para quien "[m]ediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales"[106].

En definitiva, como se podrá advertir, tanto el *skimming* como el *phishing* quedaron limitados a la existencia de un fraude. Según interpreto, allí reside una cuestión importante a tener en cuenta a la hora de determinar si estas maniobras deberían ser legisladas de manera autónoma. Si se considera que la obtención no autorizada de datos solo afecta un objeto de bien jurídico ajeno en el momento en el que estos se utilizan, por ejemplo, para cometer una defraudación, entonces la técnica legislativa elegida sería la correcta. No habría motivo alguno para sancionar la conducta en la medida en la que no

---

[102] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 2, 2019, p. 118.

[103] Sin embargo, como se explicó, la alteración del normal funcionamiento de un sistema informático o la transmisión de datos exigida dejó fuera del alcance de la norma mencionada los casos más frecuentes de *phishing* que no se materializan mediante una alteración. Además, en estos no se encuentra presente el elemento disposición patrimonial necesario para la estafa genérica. Entonces, solo se ven alcanzados por la figura del artículo 173, inciso 15, del digesto sustantivo, cuando los datos pescados y utilizados son los correspondientes a tarjetas de crédito, débito o compra. Al respecto, ver la explicación brindada en el capítulo II, apartado B, de este trabajo.

[104] Senado de la Nación Argentina, expediente 2257/11, fecha de ingreso 09/09/2011 y caducidad 28/02/2013 (https://www.senado.gob.ar/parlamentario/comisiones/verExp/2257.11/S/PL, consultado el 9 de enero de 2021).

[105] Senado de la Nación Argentina, expediente 1312/12, fecha de ingreso 15/05/2012 y caducidad 28/02/2014 (https://www.senado.gob.ar/parlamentario/comisiones/verExp/1312.12/S/PL, consultado el 10 de enero de 2021). En rigor, este proyecto proponía tipificar el delito de suplantación de identidad digital, pero incluía entre las acciones prohibidas las de adquirir y poseer datos de identificación personal, por lo que interpreto que la captación de ellos podría verse también alcanzada.

[106] Art. 123, inc. 3, apartado "d", Anteproyecto de Código Penal de la Nación, Ministerio de Justicia y Derechos Humanos de la Nación, Infojus, 2014, p. 388 (disponible en la Biblioteca Digital de dicha cartera ministerial: http://www.bibliotecadigital.gob.ar/items/show/1570, consultado el 30 de enero de 2021).

se verifique un daño patrimonial o de otro tipo. Si este fuera el caso, a lo sumo se podría corregir la redacción de algunas figuras existentes como, por ejemplo, eliminar la exigencia de la mencionada -y criticada- alteración en el artículo 173, inciso 16, del ordenamiento sustantivo. Si por el contrario se piensa que la captación de información personal es lesiva o riesgosa por sí misma, es decir, independientemente de un perjuicio patrimonial, se debe concluir que la legislación vigente es insuficiente en tanto no la prohíbe de manera autónoma ni como parte de la tentativa de otros delitos.

En este sentido, al menos a mi entender, la obtención ilícita de datos financieros personales -u otros de los alcanzados por el artículo 2.º de la Ley 25.326- afecta no solo potencialmente la propiedad sino también la privacidad[107]. Tal como indica el autor recién citado, "[e]n general, todas las leyes de protección de datos europeas limitan la libre circulación de información y penalizan de alguna forma la obtención ilícita de datos personales. Estas sanciones tienden a amparar la privacidad y no el patrimonio, pero […] el robo de identidad es un delito que principia con la obtención de datos personales (de allí que ataque la privacidad y la protección de datos) con la finalidad de perjudicar el patrimonio"[108]. En definitiva, más allá de que es cierto que dichas maniobras buscan generalmente lograr un beneficio patrimonial, no se debe perder de vista que las mismas implican por sí solas un ataque a datos personales, privados y confidenciales como pueden ser los de tarjetas bancarias. A todo evento, si en virtud del artículo 153 del Código Penal se encuentra prohibido abrir o acceder indebidamente a una carta o comunicación electrónica -no dirigida al autor-, razonablemente también debería estarlo el obtener otros datos secretos como los bancarios. En estos términos, la existencia de una norma que sancione las conductas en cuestión, independientemente de un ulterior daño a la propiedad, sería razonable.

Por otro lado, también a favor de la idea de que la captación de datos se tipifique independientemente de los casos especiales de estafa mencionados, se debe tener presente que las maniobras en cuestión pueden ser llevadas a cabo sin la finalidad de cometer un

[107] En referencia al *phishing* como ejemplo de robo de identidad, PALAZZI sostiene que, además de la privacidad y la propiedad, se afecta el honor, en tanto la víctima, una vez perpetrado el ataque al patrimonio, figurará como deudora "en registros de morosos sobre la base de una obligación que nunca contrajo" (PALAZZI, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 2016 [2009], p. 166). Aunque en términos generales coincido con la afirmación del autor, considero importante destacar que si los casos de obtención ilegítima de datos personales derivan en una afectación al honor y la propiedad es porque ya existió una violación a la privacidad de la persona.

[108] PALAZZI, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 2016 [2009], p. 168 y sus citas.

fraude sino de obtener un beneficio económico por su venta -por ejemplo, en mercados negros digitales-. En este sentido, dado que la venta de información personal tampoco se encuentra penalizada, he intentado demostrar que las acciones de pescar y vender datos quedarían limitadas -aunque es discutible- a una colaboración en el hecho delictivo principal que comete otro y, en el caso, este debería iniciar su ejecución para que el aporte del pescador tome relevancia jurídico-penal. Por los mismos motivos y por ser las modalidades de captación de datos aquí analizadas actos preparatorios respecto del fraude con tarjetas, he también explicado que tampoco sería posible una imputación en los términos del artículo 210 del código de fondo en supuestos en los que tres o más personas se organizaran con el fin de obtener y vender datos de tarjetas bancarias u otros personales. En resumen, captar y vender información personal, privada y confidencial de las personas no sería merecedor de una pena si no se concreta otro delito posterior. Mientras esto último no ocurra, las acciones en cuestión escapan al ámbito de lo prohibido según nuestra legislación vigente.

A su vez, así como la obtención y venta de datos es atípica, también lo será su compra posterior. En este sentido, resulta conveniente que se tipifiquen, además de la acción de obtener ilegítimamente dicha información, las conductas de venderla y adquirirla. Legislar únicamente el primer tramo (la captación) podría ser insuficiente. Nótese que, aun si existiera un tipo penal que prohíba dicha captación, la persona que posteriormente adquiriera -por ejemplo, a cambio de dinero- los datos pescados no estaría cometiendo un encubrimiento en los términos del artículo 277, inciso 1, apartado "c", del Código Penal, que se refiere expresamente a las hipótesis de adquirir, recibir u ocultar dinero, cosas o efectos -provenientes de un delito-, de modo que, como puede verse, los datos que aquí interesan no quedan comprendidos entre los objetos de la acción.

Asimismo, es dable mencionar que las maniobras de obtención de datos como el *phishing* "son el primer eslabón en la cadena de gran parte de los delitos informáticos"[109]. En este sentido, estos autores proponen "la punición de las actividades relacionadas a la captura ilegítima de información, por considerarse que ello sería atacar un aspecto medular del cibercrimen, toda vez que tender hacia su mitigación sería tomar una medida de importantes consecuencias en la disminución de otros delitos informáticos de mayor

[109] TEMPERINI/BORGHELLO, "La captación ilegítima de datos confidenciales como delito informático en Argentina", en Simposio de Informática y Derecho. Jornadas Argentinas de Informática n.° 41, 2012, ISSN: 1850-2814, p.106 (http://41jaiio.sadio.org.ar/sites/default/files/8_SID_2012.pdf, consultado el 9 de enero de 2021).

complejidad"[110]. En la misma dirección, se ha dicho que "los actos preparatorios como la captación de datos personales, de imagen o económico-financieros con el fin de causar perjuicios, debe penalizarse autónomamente, aun cuando no hayan sido obtenidos vulnerando claves de acceso a las cuentas"[111], y que "sería recomendable la sanción penal también para la compilación, venta e intercambio, mediante cualquier tipo de comunicación, de credenciales de usuarios o datos de tipo personal"[112].

Por las razones expuestas, considero que la obtención ilícita de datos financieros personales -u otros- debe ser legislada de manera independiente de los casos especiales de estafa analizados. Dicha captación de información significa un ataque a datos privados y confidenciales que, aunque puede derivar en la producción de daños patrimoniales (estafa, extorsión, etc.), es también realizada con otros fines disvaliosos que escapan al ámbito de lo prohibido por nuestra legislación (v.gr., venta y compra de datos). De este modo, entiendo que se justifica el adelantamiento de su punición -como delito de peligro abstracto- para prevenir ese primer paso clave en la comisión de otras conductas delictivas. Volveré sobre esta cuestión al final del capítulo.

Ahora bien, ¿sería adecuado que dichas maniobras sean reguladas como contravenciones y no como delitos? Según interpreto, existen -al menos- dos motivos por los cuales resultaría conveniente rechazar esa propuesta y, en cambio, tipificarlas como delitos autónomos.

Por un lado, las contravenciones, como tales, deben ser establecidas por las legislaturas locales y, en función de ello, su tipificación puede variar en cada jurisdicción. La dispersión que ello generaría -y que se evitaría de tratarse de un delito incorporado al Código Penal por una ley del Congreso de la Nación- podría llevar a problemas como,

---

[110] TEMPERINI/BORGHELLO, "La captación ilegítima de datos confidenciales como delito informático en Argentina", en Simposio de Informática y Derecho. Jornadas Argentinas de Informática n.° 41, 2012, ISSN: 1850-2814, pp.106 y 107 (http://41jaiio.sadio.org.ar/sites/default/files/8_SID_2012.pdf, consultado el 9 de enero de 2021). Es dable señalar que, según los autores citados, Argentina debería tipificar la captación ilegítima de datos confidenciales en consonancia con lo establecido en el artículo 6 del Convenio de Budapest sobre cibercrimen.

[111] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "A diez años de la ley de delitos informáticos. Balances y propuestas", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 1, 2019, p. 159. También a favor de la tipificación del *phishing* se han manifestado en el XIX Congreso Internacional de Derecho Penal de la Asociación Internacional de Derecho Penal, celebrado en Río de Janeiro entre el 31 de agosto y el 6 de septiembre de 2014. Entre sus conclusiones se expresa: "El robo de identidad, incluido el llevado a cabo a través de *phishing*, en su conjunto o en sus componentes, debe ser tipificado, si no se dispone lo contrario por otras disposiciones penales. Si los Estados optan por criminalizar la mera posesión de información relacionada con la identidad o hacerse pasar por personas no existentes, deben limitarse a los actos cometidos con intención criminal de causar daño…" (DE LUCA, "Delitos informáticos, apuntes de 2016", en DUPUY/KIEFER, *Cibercrimen*, t. I, 2020, p. 23).

[112] CHERÑAVSKY/GRIS MUNIAGURRIA/MOREIRA, "A diez años de la ley de delitos informáticos. Balances y propuestas", en RIQUERT (Dir.)/ SUEIRO (Coord.), *Sistema penal e informática*, tomo 1, 2019, p. 159.

por ejemplo, que una persona realice una de las conductas en cuestión desde un lugar en el que no se encuentre contemplada. Esto toma especial relevancia si se tiene en cuenta que las maniobras de captación de datos pueden realizarse a distancia, desde una a otra parte del país.

Por otro lado, una de las características principales de los delitos informáticos o cometidos por medios informáticos es su transnacionalidad. Los avances tecnológicos permiten que estos sean llevados a cabo en múltiples jurisdicciones sin necesitar mucho más que una conexión a Internet. En este sentido, lograr una colaboración internacional eficaz, particularmente en materia probatoria, se torna esencial a los fines de la investigación de los mismos. Pero además de estas cuestiones, advierto que no legislar ciertas conductas -como, en lo que aquí interesa, la obtención ilícita de datos- se traduciría en obstáculos también para su persecución y juzgamiento. En materia de extradición, los tratados exigen generalmente que el hecho por el cual esta se reclama constituya un delito y sea punible por las leyes de los estados -requerido y requirente- con un monto de pena determinado[113]. Entonces, la prevención, persecución y juzgamiento de las maniobras bajo análisis demandan reformas legislativas en materia penal, no solo en Argentina sino a nivel global.

Del análisis del derecho comparado se advierte que otros países han previsto de una u otra forma en sus legislaciones sanciones para la obtención ilícita de datos. A modo de ejemplo, en Colombia, mediante la sanción de la Ley 1273 del año 2009, se incorporó al Código Penal el título VII bis denominado "De la protección de la información y de los datos", cuyo capítulo primero reza "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". En este último se encuentra el artículo 269G, que en su primera parte establece: "Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más

[113] En este sentido y a modo de ejemplo, art. 6 de la Ley 24.767, art. 1, inc. b, del Tratado Interamericano de Extradición (ratificado por Decreto/Ley 1638/1956), art. 2, inc. 1, del Tratado de Extradición entre la República Argentina y los Estados Unidos Mexicanos (aprobado por Ley 26.867), art. 2, inc. 1, del Tratado de Extradición entre la República Argentina y la República de Sudáfrica (aprobado por Ley 26.972), entre otros.

grave…"[114]. A su vez, el artículo 269H prevé entre las circunstancias agravantes, por ejemplo, revelar o dar a conocer el contenido de la información en perjuicio de otro (inc. 4 de dicho artículo).

De forma más específica, varios estados de los Estados Unidos de América previeron normas contra el *phishing*[115]. A modo de ejemplo, el Código de Virginia establece: "§ 18.2-152.5:1. El uso de una computadora para recopilar información identificatoria; sanciones. A. Es ilegal que cualquier persona, que no sea un funcionario encargado del cumplimiento de la ley, como se lo define en el artículo § 9.1-101, y que actúa en el desempeño de sus funciones oficiales, utilice una computadora para obtener, acceder, o registrar, mediante el uso de artificio, ardid o engaño, cualquier información identificatoria, como se define en cláusulas (iii) a (xiii) del inciso C del articulo § 18.2-186.3. Cualquier persona que infrinja lo dispuesto en este articulo será considerada culpable de un delito mayor de Clase 6. B. Cualquier persona que infrinja lo dispuesto en este articulo y venda o distribuya dicha información será considerada culpable de un delito mayor de Clase 5. C. Cualquier persona que infrinja lo dispuesto en este articulo y utilice dicha información en la comisión de otro delito será considerada culpable de un delito mayor de Clase 5"[116]. Por su parte, en los Estatutos de Minnesota se prevé: "Subd. 5a. Delito de uso electrónico de declaraciones fraudulentas para obtener identidad. (a) Una persona que, con la intención de obtener la identidad de otra, utiliza declaraciones engañosas en un correo electrónico para otra persona o en una página web, comunicación electrónica, publicidad o en cualquier otra comunicación a través de Internet, será considerada culpable de un delito"[117]. También se prohiben maniobras de *skimming*, al establecerse: "Subd. 5b. La posesión o utilización ilegítima de un dispositivo de escaneo o de clonación de información. (a) Una persona que utiliza un dispositivo de escaneo o de clonación/codificación de información sin la autorización del titular de la tarjeta desde la cual la información está siendo escaneada o clonada/codificada, con la intención de

[114] Ley 1273 de la República de Colombia, del 5 de enero de 2009 (disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf, consultado el 9 de enero de 2021).
[115] Para acceder a la legislación de cada uno de esos estados, se sugiere compulsar el sitio *web* de la Conferencia Nacional de Legislaturas Estatales -o N.C.S.L., por sus siglas en inglés-, que compila las normas que abordan el *phishing* (https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx, consultado el 10 de enero de 2021).
[116] Código de Virginia, § 18.2-152.5:1 (https://law.lis.virginia.gov/vacode/title18.2/chapter5/section18.2-152.5:1/, consultado el 11 de enero de 2021). La información que es objeto de estas disposiciones, según las cláusulas allí mencionadas, incluye datos bancarios como los de tarjetas de crédito o débito. Aclaro que he realizado personalmente tanto esta como las siguientes traducciones del idioma inglés.
[117] Estatutos de Minnesota, artículo 609.527, inciso 5a https://www.revisor.mn.gov/statutes/cite/609.527#stat.609.527.5a, consultado el 11 de enero de 2021).

cometer, cooperar o instigar cualquier actividad ilícita, será considerada culpable de un delito"[118].

En nuestro país, además de los intentos de reformas ya mencionados, es dable señalar que el último Proyecto de Ley de Reforma al Código Penal contempla la obtención ilegítima y venta de datos de manera autónoma. Así, en su artículo 491 establece: "Se impondrá prisión de seis meses a dos años o seis a veinticuatro días-multa, al que ilegítimamente con ánimo de lucro o la finalidad de cometer un delito, y valiéndose de alguna manipulación informática, ardid o engaño, obtuviere claves o datos personales, financieros o confidenciales de un tercero, siempre que el hecho no constituya un delito más severamente penado. La misma pena se impondrá a quien compilare, vendiere, intercambiare u ofreciere, de cualquier manera, claves o datos de los mencionados en el primer párrafo"[119]. Aunque, como a continuación explicaré, no comparto la técnica legislativa escogida, advierto que quizá sería conveniente que, en este último supuesto, se agregara la prohibición del que "adquiriere o recibiere" la información en cuestión, pues, aunque el término "intercambiare" incluiría a dos o más personas (en el caso, vendedor y comprador), las acciones aquí sugeridas resultan más precisas. Además, escaparía a dicha norma el caso de quien recibe los datos captados sin dar nada a cambio -por ejemplo, porque se los obsequian-.

Según interpreto, sería preferente evitar la estructura de "delito mutilado de dos actos"[120] y, de ese modo, los problemas que se pueden presentar para probar la "finalidad de cometer un delito". En cambio, entiendo que, si lo que se busca es adelantar la punición para prevenir esos primeros momentos claves en la comisión de otras conductas disvaliosas, basta con prohibirlos sin exigir un elemento subjetivo distinto del dolo. A todo evento, resulta conveniente mantener una conminación penal relativamente leve porque, al tratarse de delitos de peligro abstracto, "la escala penal debe ser adecuada al contenido de ilícito claramente reducido en comparación con el correspondiente delito de lesión o de peligro concreto"[121]. En definitiva, podría pensarse en la siguiente formulación: "Será reprimido con prisión de un mes a un año: a) el que, mediante

---

[118] Estatutos de Minnesota, artículo 609.527, inciso 5b https://www.revisor.mn.gov/statutes/cite/609.527#stat.609.527.5a, consultado el 11 de enero de 2021).

[119] Proyecto de Ley de Reforma al Código Penal, Senado de la Nación Argentina, expediente 52/19, fecha de ingreso 25/03/2019 (https://www.senado.gob.ar/parlamentario/comisiones/verExp/52.19/PE/PL, consultado el 9 de enero de 2021).

[120] MIR PUIG, *Derecho Penal. Parte General*, 2016 [1984], p. 235; ROXIN, *Derecho Penal Parte General*, t. II, 2019 [2014], p. 317.

[121] FRISTER, *Derecho Penal. Parte General*, 2016 [2006], p. 85.

dispositivos técnicos, manipulación informática, ardid, engaño, o cualquier otra modalidad ilegítima, obtuviere datos personales, bancarios, financieros o confidenciales de otra persona; b) el que, por cualquier medio, entregare, vendiere, recibiere o adquiriere ilegítimamente los datos mencionados en el inciso anterior"[122].

VI. ¿Hacia la incorporación de un nuevo tipo penal?

Los avances tecnológicos han traído a la sociedad, además de innumerables beneficios, riesgos antes impensados. En la introducción de este trabajo, sugerí la necesidad de analizar, ante la velocidad con la que crecen las tecnologías y los delitos vinculados a estas, si nuestro ordenamiento jurídico responde a tal dinamismo y, en caso afirmativo, si lo hace de manera adecuada. En particular, me he detenido, en el marco de la Parte Especial del Derecho Penal y dentro de los delitos contra la propiedad, en las formas modernas de defraudación en cuya comisión se utiliza la tecnología. En concreto, propuse analizar si las maniobras de obtención de datos de tarjetas de crédito y débito u otros -puntualmente, *skimming* y *phishing*- constituyen actos preparatorios o ejecutivos de la posterior defraudación cometida mediante tarjetas falsificadas y/o el uso no autorizado de sus datos.

Tras repasar cómo se suele resolver la cuestión a nivel jurisprudencial, expliqué, a partir del análisis de casos que elaboré al efecto, que dichas maniobras son actos preparatorios y, por ende, no revisten el carácter de ejecutivos de esos casos especiales de estafa ni de la falsificación de tarjetas prevista en el artículo 282, en función del 285, del Código Penal. Entonces, dado que ambas modalidades de captación de datos fueron legisladas única e indirectamente a través de dichas defraudaciones (leyes 25.930 y 26.388), el *skimming* solo puede ser subsumido en el artículo 299 del código de fondo, mientras que el *phishing* es atípico. En este sentido, en la medida en la que el pescador de datos se limite a, valga la redundancia, pescarlos, no realiza una conducta penalmente relevante.

[122] Como se podrá advertir, se establece una pena de prisión relativamente menor a la del proyecto recién citado. Ello dado que, desde una interpretación sistemática, considero erróneo que la escala penal allí propuesta (seis meses a dos años) tenga, por ejemplo, el mismo máximo -y un mínimo mayor- que el hurto del art. 162 del C.P. En cambio, entiendo que es preferible imponer una pena más leve como la aquí sugerida, que resulta ser algo mayor a la del art. 153 y menor a la del art. 157 bis del C.P. Por otro lado, la presencia del elemento normativo por el que se exige que las acciones típicas sean realizadas de manera ilegítima, procura excluir conductas lícitas relativas al tratamiento autorizado de datos personales, financieros, entre otros.

Asimismo, en el desarrollo del análisis advertí que, dado que la venta de información personal tampoco se encuentra penalizada, las acciones de pescar y vender datos quedarían limitadas a una posible colaboración en el hecho delictivo principal que comete otro y, en el caso, este debería iniciar la ejecución del mismo para que el aporte del pescador tome relevancia jurídico-penal. A su vez, expliqué que tampoco sería posible una imputación en los términos del artículo 210 del código de fondo en supuestos en los que tres o más personas se organizaran con el fin de obtener y vender datos de tarjetas bancarias u otros personales, en tanto la norma exige que dicha asociación se encuentre destinada a cometer delitos. En resumen, concluí que, según nuestra legislación vigente, captar y vender información personal, privada y confidencial de las personas no sería *per se* merecedor de una pena.

Tras responder al primer y principal interrogante sobre el que giró este trabajo, planteé si la obtención ilegítima de datos financieros personales debería tipificarse de manera autónoma, adelantando la penalidad. A ese fin, habiendo explicado que las maniobras en cuestión no constituyen el comienzo de ejecución desde la perspectiva de los casos especiales de estafa ni de la falsificación de tarjetas, brindé argumentos a favor de la creación de un tipo penal de adelantamiento para dichas conductas.

En este sentido, advertí que la obtención no autorizada de datos personales, privados y confidenciales afecta no solo potencialmente la propiedad sino también la privacidad. A su vez, que esta clase de maniobras no son únicamente realizadas con la finalidad de cometer una defraudación sino también otros delitos, o incluso con la de vender la información captada. Sin embargo, según nuestra legislación vigente, no es posible sancionar ni la pesca ni la venta de datos (tampoco su adquisición), en tanto no se ejecute otro injusto respecto del que, tal vez, puedan ser consideradas aportes típicos.

Nuestra legislación penal parece aún no haberse adaptado adecuadamente a la evolución de la tecnología cuando, como se señaló, sí lo ha hecho la de otros países. El análisis del derecho comparado evidencia que en otros estados se ha intentado, de una u otra forma, tipificar la obtención ilegítima de datos personales -por ejemplo, mediante *phishing*-. En estos términos, resulta conveniente la incorporación al Código Penal de una fórmula típica para las acciones de captación, venta y adquisición de dicha información. Elaborar una propuesta de reforma legislativa como la sugerida en el capítulo anterior puede haber sido algo pretencioso para un trabajo con los límites de extensión del presente. Pero entiendo que, cuanto menos, los argumentos desarrollados en estas páginas podrían ser de utilidad para una futura modificación al ordenamiento sustantivo.

Seguramente, la prevención de las maniobras aquí analizadas -lesivas o riesgosas por sí mismas, independientemente de ulteriores delitos- demande más que modificaciones legislativas, pero estas se presentan como imperiosas.

Bibliografía

ABOSO, Gustavo Eduardo, *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, reimpr., BdeF, Montevideo-Buenos Aires, 2020 [2017].

BACIGALUPO, Enrique, *Estudios sobre la parte especial del derecho penal*, Akal, Madrid, 1991.

BUOMPADRE, Jorge E., "Estafas y otras defraudaciones" en BAIGÚN, David (Dir.)/ZAFFARONI, Eugenio R. (Dir.)/TERRAGNI, Marco A. (Coord.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, t. 7, Hammurabi, Buenos Aires, 2009, pp. 43/301.

CHERÑAVSKY, Nora/GRIS MUNIAGURRIA, Pablo H./MOREIRA, Diógenes A., "A diez años de la ley de delitos informáticos. Balances y propuestas", en RIQUERT, Marcelo A. (Dir.)/SUEIRO, Carlos Christian (Coord.), *Sistema penal e informática*, t. 1, Hammurabi, Buenos Aires, 2019, pp. 129/160.

CHERÑAVSKY, Nora/GRIS MUNIAGURRIA, Pablo H./MOREIRA, Diógenes A., "«Phishing»: abordaje del fenómeno desde la prevención y la investigación", en RIQUERT, Marcelo A. (Dir.)/SUEIRO, Carlos Christian (Coord.), *Sistema penal e informática*, t. 2, Hammurabi, Buenos Aires, 2019, pp. 117/134.

D'ALESSIO, Andrés José (Dir.)/DIVITO, Mauro Antonio (Coord.), *Código Penal de la Nación comentado y anotado*, 2.ª ed. actualizada y ampliada, 1.ª reimpresión, La Ley, Buenos Aires, 2011 [2004/2005].

DE LUCA, Javier Augusto, "Delitos informáticos, apuntes de 2016", en DUPUY, Daniela/KIEFER, Mariana, *Cibercrimen*, t. I, BdeF, Montevideo-Buenos Aires, 2020, pp. 7/32.

DONNA, Edgardo Alberto, *Delitos contra la propiedad*, 3.ª ed. ampliada, Rubinzal-Culzoni, Santa Fe, 2016 [2001].

FRISTER, Helmut, *Derecho Penal. Parte General* (traducción de Marcelo A. SANCINETTI), 4.ª ed., 1.ª reimpr., Hammurabi, Buenos Aires, 2016 [2006].

GARAT, Sebastián/REALE, Julián, "La reforma penal en materia de cibercrimen en la República Argentina", en DUPUY, Daniela/KIEFER, Mariana, *Cibercrimen*, t. II, BdeF, Montevideo-Buenos Aires, 2020, pp. 485/529.

GOTTHEIL, Diego F./LÓPEZ, Santiago A., "Nuevos delitos vinculados con tarjetas (A propósito de las modificaciones al Código Penal introducidas por la ley 25930)", en *Revista de Derecho Penal y Procesal Penal*, vol. 4, Lexis Nexis, 2004, pp. 727/734.

JAKOBS, Günther, *Derecho Penal. Parte General. Fundamentos y teoría de la imputación* (trad. Joaquín CUELLO CONTRERAS y José Luis SERRANO GONZÁLEZ DE MURILLO), 2.ª ed. corregida, Marcial Pons, Madrid, 1997 [1983].

JESCHECK, Hans-Heinrich/WEIGEND, Thomas, *Tratado de Derecho Penal. Parte General* (traducción de Miguel OLMEDO CARDENETE), 5.ª ed., Comares, Granada, 2002.

MAURACH, Reinhart/GÖSSEL, Karl Heinz/ZIPF, Heinz, *Derecho penal. Parte general* (traducción de Jorge BOFILL GENZSCH), t. II, 7.ª ed., Astrea, Buenos Aires, 1995.

MIR PUIG, Santiago, *Derecho Penal. Parte General*, 10.ª ed., BdeF, Montevideo-Buenos Aires, 2016 [1984].

MIRÓ LLINARES, Fernando/GÓMEZ BELLVÍS, Ana Belén, "La estafa informática: fenomenología y respuesta jurídica", en DUPUY, Daniela/KIEFER, Mariana, *Cibercrimen*, t. II, BdeF, Montevideo-Buenos Aires, 2020, pp. 5/36.

MUÑOZ CONDE, Francisco/GARCÍA ARÁN, Mercedes, *Derecho Penal, Parte General*, 9.ª ed., Ed. Tirant lo Blanch, Valencia, 2015 [1993].

NÚÑEZ, Ricardo C., *Tratado de Derecho Penal*, t. IV, Ediciones Lerner, Córdoba-Buenos Aires, 1978.

PALAZZI, Pablo Andrés, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 3.ª ed., Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2016 [2009].

PESSOA, Nelson R., *La tentativa. Distinción entre actos preparatorios y actos de ejecución de delitos*, 2.ª ed., Hammurabi, Buenos Aires, 1998 [1987].

PETRONE, Daniel/BASSO, Marina/EMILIOZZI, Agustina, "*Phishing attacks:* Problemáticas de su recepción en el ordenamiento local y nuevos desafíos", en DUPUY, Daniela/KIEFER, Mariana, *Cibercrimen*, t. I, BdeF, Montevideo-Buenos Aires, 2020, pp. 277/290.

RIGHI, Esteban, *Delito de estafa*, 2.ª ed., Hammurabi, Buenos Aires, 2017 [2015].

ROXIN, Claus, *Derecho Penal Parte General* (traducción de Diego-Manuel LUZÓN PEÑA, Miguel DÍAZ Y GARCÍA CONLLEDO, José Manuel PAREDES CASTAÑÓN, Javier de VICENTE REMESAL y otros), t. II, 3.ª reimpr., Thomson Reuters-Civitas, Buenos Aires, 2019 [2014].

SALLIS, Ezequiel, "Desafíos de la investigación de los delitos informáticos en la "*Deep & Dark Web*", en DUPUY, Daniela/KIEFER, Mariana, *Cibercrimen*, t. I, BdeF, Montevideo-Buenos Aires, 2020, pp. 601/616.

SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho Penal*, 3.ª ed., BdeF, Montevideo-Buenos Aires, 2011 [1999].

SOLER, Sebastián, *Derecho Penal Argentino*, t. V, La Ley, Buenos Aires, 1946

TEMPERINI, Marcelo/MACEDO, Maximiliano, "Aspectos legales de la ingeniería social: análisis sobre la responsabilidad civil y penal del ingeniero social", en RIQUERT, Marcelo A. (Dir.)/ SUEIRO, Carlos Christian (Coord.), *Sistema penal e informática*, t. 3, Hammurabi, Buenos Aires, 2020, pp. 67/90.

TEMPERINI, Marcelo/BORGHELLO, Cristian, "La captación ilegítima de datos confidenciales como delito informático en Argentina", en Simposio de Informática y Derecho. Jornadas Argentinas de Informática n.° 41, 2012, ISSN: 1850-2814, pp. 94/108 (http://41jaiio.sadio.org.ar/sites/default/files/8_SID_2012.pdf)

TOSELLI, Nicolás/NICOLOSI LÓPEZ, Juan M./CHOUELA, Diego A., "Nuevas formas de defraudación: *phishing*", en *Revista de Derecho Penal y Procesal Penal*, vol. 2, Lexis Nexis, 2007, pp. 307/313.

VANINETTI, Hugo Alfredo/VANINETTI, Gustavo Juan, "Estafa en Internet", en *El Derecho - Diario*, tomo 211, 2005, p. 679 (cita digital ED-DCCLXVII-336, 14 de febrero de 2005).

VANINETTI, Hugo Alfredo/VANINETTI, Gustavo Juan, "Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet", en *El Derecho - Diario*, tomo 229, 2008, p. 776 (cita digital ED-DCCLXX-349, 15 de septiembre de 2008).

WELZEL, Hans, *Derecho penal alemán. Parte general* (trad. Juan BUSTOS RAMÍREZ y Sergio YAÑÉZ PERES), 11.ª ed. (4.ª ed. en español), Editorial Jurídica de Chile, Santiago, 1970.

ZAFFARONI, Eugenio Raúl/SLOKAR, Alejandro/ALAGIA, Alejandro, *Manual de Derecho Penal: parte general*, 2.ª ed., 8.ª reimpresión, Ediar, Buenos Aires, 2014 [2005].