Proliferación de ciberfraudes: a propósito de los incisos 15 y 16 del artículo 173 del Código Penal de la Nación

Proliferation of cyberfrauds: regarding paragraphs 15 and 16 of article 173 of the Criminal Code of the Nation

Director y coautor: Ricardo Levene (nieto)[*]

Coautores: Dres. Agustín Orfila, Francisco Cassotto, Federico Trotta, Valeria Besansón (coordinadora) y Horacio Adrián Garrofe[**]

RESUMEN

El avance tecnológico y su aceleración a raíz de la pandemia de COVID-19 habilitó un lugar para que nuevos delitos telemáticos sean cometidos. El ingreso al Código Penal argentino de los incisos 15 y 16 del artículo 173 ha posibilitado la tipificación específica de este tipo de conductas —utilización fraudulenta de tarjetas, uso no autorizado de datos, estafas informáticas, entre otros—, que tienen vinculación directa con la obtención ilegal de datos sensibles en desmedro del patrimonio de las personas.

Palabras clave: avances tecnológicos, ciberfraudes, Código Penal, datos sensibles

ABSTRACT

Technological advance and its acceleration as a result of the COVID-19 pandemic, enabled a place for new telematic crimes to be committed. The entry into the Argentine Penal Code of sections 15 and 16 of article 173, has made possible the specific classification of this type of conduct - fraudulent use of cards, unauthorized use of data,

[*] Profesor emérito de Derecho Penal, Facultad de Ciencias Jurídicas, Universidad del Salvador.

[**]Profesores auxiliares de la cátedra de Derecho Penal II —parte especial— a cargo del Dr. Ricardo Levene (nieto), en la Facultad de Ciencias Jurídicas de la Universidad del Salvador.

computer scams, among others - that are directly linked to the illegal obtaining of sensitive data to the detriment of people's assets.

Keywords: Technological advances, cyberfrauds, Criminal Code, sensitive data

I. Introducción

Al momento de celebrarse el VI Congreso Latinoamericano en 1998[1], en Colonia, República Oriental del Uruguay, se alertaba acerca de que los delitos informáticos ocuparían un lugar estelar en la criminalidad de un futuro cercano. También se pronosticó que la economía se desarrollaría en un plano virtual y que el concepto de intimidad se vería modificado. Aquellos presagios que parecían lejanos, desde hace un tiempo se han convertido en una realidad.

Para aquella misma época, adelantándose a lo que estaba por venir, el Dr. Ricardo Levene (nieto) —profesor Emérito de esta cátedra—, junto con la Dra. Alicia Chiaravalloti (1998), alertaron a la comunidad jurídica: "El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas" (p. 1).

En efecto, los mencionados juristas (1998) advirtieron acertadamente para ese entonces que

> El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho […] Desde la

[1] VI Congreso Latinoamericano de "Tipos de Delitos Informáticos", organizado por la Organización de las Naciones Unidas en 1998, en la ciudad de Colonia, Uruguay.

> criminología debemos señalar que anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley (p. 1).

Así fue como el inicio de la era o revolución tecnológica acarreó numerosos cambios en la vida cotidiana. Pasamos a tener perfiles digitales para utilizar redes sociales, foros, realizar operaciones bancarias, entre otros infinitos modos de interacción posibles con la web. Los activos también pasaron a digitalizarse: desde fotografías, artículos, libros; incluso hasta el patrimonio a partir de la llegada de las criptomonedas. En definitiva, nuestra información personal y propiedad han sufrido una metamorfosis completa.

Este cuadro complejo impuso al legislador la necesidad de adecuar los distintos ordenamientos para prever nuevas situaciones. Así fue como en el año 2004 se modificó el tradicional catálogo de defraudaciones contenidas en el Código Penal para introducir las cometidas mediante el uso de tarjetas de compra, débito y crédito o el uso no autorizado de datos. En 2008 llegaría una gran reforma y se incluirían las realizadas por cualquier técnica de manipulación informática que alterase el normal funcionamiento de un sistema informático o la transmisión de datos.

Asimismo, incluyó la ampliación de las conductas relacionadas con la pornografía infantil, la inserción de la comunicación electrónica como forma de violación de la privacidad, su publicación y la sanción del ingreso indebido a un sistema informático de acceso restringido o de un banco de datos personales.

Cabe aclarar que, tiempo antes de que se llevaran a cabo dichas reformas en el ámbito local, el Consejo de Europa había celebrado el Convenio de Budapest —también

conocido como Convenio sobre la Ciberdelincuencia—[2] a través del cual los Estados parte se comprometieron a cooperar en la prevención, investigación y sanción de delitos informáticos. Y si bien es cierto, conforme se expuso, que nuestro país había incorporado las conductas que allí se recomendaba tipificar, no lo es menos que ratificaría dicho tratado casi dos décadas después[3], lo que denota la tardía importancia otorgada a la materia.

Este panorama no deja dudas en cuanto a que el flagelo de la ciberdelincuencia era una problemática que afrontaba el mundo, pero que se acrecentaría exponencialmente a partir de la crisis pandémica originada por el SARS-CoV2-19. Ello traería aparejado que a nivel global se dispusieran aislamientos preventivos en casi todas las sociedades que implicaron, como hemos vivido, la restricción para realizar actividades presenciales.

Consecuentemente, la mayoría de las diligencias se convirtieron en virtuales y, entre otras cosas, las operaciones digitales pasaron a ser el único medio por el cual se podían adquirir bienes y servicios. Así, se impuso la necesidad de operar mediante medios electrónicos y de engrosar la cartera de clientes que, hasta ese momento no se hallaban bancarizados o no operaban de esa manera. Por supuesto, dicha circunstancia generó el auge de la criminalidad digital, lo que desató un crecimiento exponencial de denuncias, al igual que el desarrollo y la mejora de las modalidades engañosas para hacerse de datos personales, vitales para lograr el designio criminal[4].

---

[2] Suscripto el 23 de noviembre de 2001 en Budapest, Hungría, por los Estados miembros del Consejo de Europa.

[3] El Convenio de Budapest fue aprobado e incorporado a la legislación nacional el 22 de noviembre de 2017 a través de la ley 27411 con las reservas que se mencionan en su artículo segundo.

[4] Véase la siguiente noticia publicada en uno de los diarios digitales de mayor circulación del país respecto del aumento de los ciberfraudes: https://tn.com.ar/tecno/novedades/2021/11/07/tendencias-en-ciberdelito-mas-del-50-de-los-bancos-a-nivel-mundial-experimentaron-aumentos-en-la-cantidad-y monto-de-fraudes

Dicha afirmación se ve corroborada mediante las alarmantes estadísticas expuestas por el titular de la Unidad Fiscal Especializada en Ciberdelincuencia, Horacio Azzolin (2021), quien aseveró que

> comparando marzo 2019 a marzo 2020 y marzo 2020 a marzo 2021 pasamos de 2.581 denuncias a recibir un total de 14.583. El aumento, en términos porcentuales, corresponde a un 465%. En cuanto a denuncias pasamos de 1.305 casos de fraude a 8.559, lo que representa un 58,7% aproximadamente del total de los casos y cerca de 50 denuncias diarias. De accesos a cuentas, pasamos de 229 a 1.220[5].

Bajo el panorama expuesto entendemos oportuno analizar y efectuar algunas consideraciones acerca de los aludidos tipos penales de estafas virtuales, como así también respecto de las modalidades más comunes que los delincuentes utilizan para obtener datos ilegalmente, entre las que se destacan el *phishing*, *pharming* y *skimming*.

II. Utilización fraudulenta de tarjetas de compra, crédito o débito. Operaciones mediante el uso no autorizado de sus datos (artículo 173, inciso 15, del Código Penal de la Nación)

Con motivo de la dificultad que ocasionaba la ausencia de una normativa específica, el legislador concluyó en el dictado de la ley 25930, por la cual incorporó el inciso 15 al art. 173 del Código Penal[6], que reprime el uso fraudulento de una tarjeta de compra, crédito o débito, y el uso no autorizado de sus datos. Así se considera un caso especial de defraudación:

[5] Según publicación del Diario Clarín, sección Tecnología, del 03/06/21 por Juan Brodersen.
[6] Publicada en el Boletín Oficial el 21 de septiembre de 2004.

> El que defraudare 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.

Como se advierte, el bien jurídico protegido es la propiedad, específicamente el patrimonio, extremo que se condice con la inclusión de esta protección normativa junto a otros casos particulares de defraudación previstos en el artículo 173 del código sustantivo. Además, esta norma trae una innovación en la dinámica de las estafas, pues incorpora un tipo penal en el que la disposición patrimonial perjudicial no se genera a partir del error en la víctima, sino por la utilización ilegal o irregular de una tarjeta de compra, crédito o débito o de sus datos en operaciones automatizadas.

En ambas alternativas que presenta el tipo penal —por un lado, la utilización no autorizada de la tarjeta en su formato físico; y, por otro, la de sus datos a través de una operación electrónica— no existen particularidades respecto de quién puede ser sujeto activo (delito común) mientras que el sujeto pasivo resulta ser el titular de la tarjeta bancaria, quien resulta perjudicado por la extracción o descuento de dinero de su cuenta personal. Sin embargo, no menos cierto es que en la mayor parte de los casos es la institución emisora de la tarjeta la que debe afrontar las erogaciones por los créditos o los débitos de la cuenta bancaria como resultado de la maniobra por el accionar defraudatorio.

La acción típica consiste entonces en defraudar, pero por medio del uso de una tarjeta de compra, crédito o débito, o mediante el uso no autorizado de datos contenidos en ellas.

Respecto de los elementos normativos del tipo, la norma protege a las denominadas tarjetas de compra, crédito o débito, todas reguladas y conceptualizadas conforme la ley 25065, que define la tarjeta de compra como "aquella que las instituciones comerciales entregan a sus clientes para realizar compras exclusivas en su establecimiento o sucursales…" (art. 2°, inc. d); a la tarjeta de crédito como "el instrumento material de identificación del usuario, que puede ser magnético o de cualquier otra tecnología, emergente de una relación contractual previa entre el titular y el emisor" (art. 4°), y a la tarjeta de débito como aquella que es entregada por las instituciones bancarias "a sus clientes para que al efectuar compras o locaciones, los importes de las mismas sean debitados directamente de una cuenta de ahorro o corriente bancaria del titular" (art. 2°, inc. e).

Materialmente las tarjetas mencionadas son documentos en soporte plástico con una banda magnética, "chip" o sistema *contactless*, que contiene los datos personales del usuario y que permite realizar operaciones bancarias.

El tipo penal requiere que el autor defraude con una tarjeta de tales características, pero "falsificada, adulterada, robada, hurtada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos". En función de ello, las alternativas típicas previstas pueden dividirse en dos grupos:

a) **Utilización fraudulenta de tarjeta de compra, crédito o débito falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño**. En este primer supuesto, lo que se sanciona es el uso indebido de las tarjetas de compra, crédito o débito que han ingresado materialmente al dominio del autor bajo alguna de las modalidades citadas, las que constituyen de por sí el "engaño o ardid" propio de esta especial clase de defraudación sin que sea necesario verificar un error en la persona física que determine la disposición patrimonial perjudicial.

Además, como se adelantó, es necesario que el instrumento ingrese al ámbito de control del autor como consecuencia de alguna de las modalidades expresamente establecidas en el tipo penal, esto es, mediante (a) la falsificación de la tarjeta; (b) la adulteración de una tarjeta original; (c) el uso de una tarjeta perdida o sustraída a su legítimo titular o usuario; y (d) la obtenida mediante ardid o engaño.

La falsificación de una tarjeta de compra, crédito o débito es aquella que resulta de la imitación de una tarjeta real emitida por quien tiene facultades para hacerlo y presenta similares elementos característicos que, razonablemente, incluye sus códigos de seguridad para que sea operativa.

La adulteración consiste en que una tarjeta de crédito, compra o débito emitida en forma legal sufra alteraciones en su sustancia y/o contenido, es decir, se modifican sus datos, por ejemplo, replicando los números de código de seguridad asignados a la tarjeta original, insertando los datos de identidad de una persona, sustituyendo la banda magnética o cualquier otro modo que signifique una alteración en su originalidad

En el caso de la utilización de una tarjeta original sustraída a su legítimo titular o usuario, la modalidad abarca tanto los supuestos donde se ejerza violencia física sobre la persona para obtener el instrumento —robo—, como aquellos donde no lo hay —hurto—. También se incluyen los casos en los que la tarjeta fue perdida y es utilizada en perjuicio del titular.

Los supuestos de obtención fraudulenta necesariamente exigen ardid o engaño suficiente por parte del sujeto activo que conduzcan a que la víctima, error mediante, le proporcione a aquel la tarjeta que luego es utilizada ilegítimamente.

b) **Uso no autorizado de datos**

En esta segunda alternativa, el sujeto activo se vale de los datos de las tarjetas de crédito, débito o compra, sin poseer materialmente el instrumento de pago ni la

autorización de su titular para utilizarla, para efectuar disposiciones de dinero perjudiciales que incluyen la operatividad a través de modalidades automáticas o electrónicas.

Lo que distingue principalmente este supuesto (b) del analizado precedentemente (a) es que el autor no tiene materialmente la tarjeta —es decir, no tiene el plástico—, sino los datos. Aquí se incluyen aquellas tarjetas en formato digital o que utilizan códigos QR.

Cabe resaltar que la inclusión de esta especial defraudación en la legislación argentina, entre otras cosas, vino a solucionar el escollo normativo que se había generado en aquellos supuestos donde el autor utilizaba los datos de una tarjeta obtenidos ilegítimamente para efectuar operaciones en perjuicio del titular, consistentes en, por ejemplo, extraer dinero de un cajero automático o pagar servicios electrónicamente.

El principal problema que generaban esos casos consistía en que el delito de estafa requería de una persona que engañase a otra, quien por error efectúa el acto de disposición patrimonial en su propio perjuicio o de un tercero, situación que era difícil de fundamentar en los casos aludidos donde la instrumentalización no recaía en la víctima sino en una máquina o sistema informático. Por ello, la nueva fórmula legal permite que el uso ilegítimo de una tarjeta represente el engaño típico del procedimiento defraudatorio sin exigir una relación directa entre dos personas.

Nótese que esta modalidad de estafa se limita específicamente a las “tarjetas de compra, crédito o débito” y a los datos obrantes en ellas, de modo que no abarca otros usos ilegítimos de datos ajenos (por ejemplo, las claves de acceso al sistema bancario móvil —*home banking*— o códigos para identificación de compra en comercios *online*). Esta omisión del legislador no está justificada y la jurisprudencia la ha cubierto al

recurrir a una interpretación amplia del concepto “manipulación informática” del art. 173, inciso 16, del Código Penal.

Por otra parte, algunas dudas ofrecen los supuestos en los que el autor está en la tenencia de la tarjeta de crédito, compra o débito con autorización de su titular para su uso, pero aquel excede abusivamente el marco del acuerdo sobre su utilización. En estos casos, no puede afirmarse que el autor haya hecho un uso no autorizado de los datos, sino respecto del alcance de la disposición del patrimonio ajeno. Por este motivo, algunos autores rechazan su aplicación dentro de este tipo penal y consideran que le es aplicable la figura de la defraudación por administración infiel (art. 173, inciso 7°, del Código Penal) (Aboso, 2007, p. 308), por ejemplo, el Dr. Levene (nieto).

En cuanto al elemento subjetivo, la figura en estudio —art. 173, inciso 15, del Código citado— se trata de un delito doloso que exige que el autor tenga conocimiento de que la tarjeta ha sido sustraída, falsificada, adulterada, obtenida de manera fraudulenta o, finalmente, que su uso no esté autorizado. Si el sujeto activo desconoce cualquiera de estos extremos, no se configura el tipo en cuestión.

En cuanto a la consumación, ocurre con la concurrencia del perjuicio patrimonial como consecuencia de alguna de la acciones o modalidades típicas. Por otro parte, la tentativa es admisible siempre que el perjuicio no se lograse perfeccionar como consecuencia de circunstancias ajenas a la voluntad del autor (por ej., entidad emisora de la tarjeta advierte el fraude y no autoriza la transacción).

En otro orden de cosas, este tipo de defraudación puede concurrir materialmente con los delitos de hurto o robo, según el caso. Además, en supuestos donde el autor realiza varias extracciones dinerarias de un cajero automático desde una misma tarjeta durante un lapso determinado se está en presencia de un hecho único, diferente a las reglas que regulan el concurso material de delitos, que no es aplicable a este supuesto.

III. Delito de defraudación informática (art. 173, inc. 16, del Código Penal de la Nación)

El art. 173, inc. 16, del Código Penal —incorporado mediante la sanción de la Ley nro. 26.388— introduce la denominada "estafa informática", conforme la cual se reprime con la pena del art. 172 al "que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

La principal distinción con la figura clásica de estafa consiste en que el error humano es reemplazado por la manipulación informática que influye sobre el proceso de tratamiento y transmisión de datos que culmina con la producción del resultado disvalioso (Pastor Muñoz, 2006, p. 219).

Esta inclusión al código de fondo busca "incorporar ciertas situaciones patrimoniales abusivas relacionadas con la informática como una modalidad de defraudación, para superar el problema que presentaba en nuestro derecho y en el comparado respecto de la imposibilidad de estafar o engañar a una máquina u ordenador" (Palazzi, 2009, p. 169).

El tipo penal de fraude informático propone innovaciones en la estructura clásica de la figura de estafa —que necesariamente exigía un error en la persona física— adaptándolas a las modalidades de los nuevos medios tecnológicos.

El bien jurídico protegido sigue siendo la propiedad, precisamente el patrimonio individual de la persona física y/o de cualquier persona jurídica. También, cabe señalar que junto al objeto de protección mencionado confluyen otros intereses subsidiariamente tutelados que se identifican con la integridad, el correcto funcionamiento y la facultad de disposición de datos.

El tipo objetivo se conforma con una modalidad abierta, es decir, el autor puede utilizar cualquier técnica de manipulación informática que implique la modificación o alteración de un proceso automatizado de datos.

La acción típica es defraudar a otro mediante una técnica de manipulación informática que produzca una alteración o modificación de un sistema de almacenamiento y/o en la transmisión de datos. Se exige que dicha injerencia provoque un funcionamiento anómalo del sistema informático, es decir, la acción del autor debe incidir sobre el proceso de funcionamiento provocando resultados inadecuados, extraños o indebidos.

La ley penal no define el concepto de "sistema de almacenamiento y tratamiento de datos", como así tampoco el significado del término "datos". En consecuencia, resulta necesario completar el tipo penal acudiendo a la Ley Nacional de Protección de Datos Personales número 25326, sancionada el 20/10/2000 y publicada en el Boletín Oficial el 2 de noviembre de ese mismo año.

Esta norma, en su art. 2 define a los "datos personales" como la "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". En el mismo artículo, respecto del **"**sistema de almacenamiento y tratamiento de datos**",** nos brinda la siguiente definición:

> Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

En palabras de Aboso (2007),

la manipulación de un programa informático es un proceso que permite la fijación de datos en la computadora. Mediante la ejecución de instrucciones, la computadora realiza una actividad que combina datos previamente almacenados. Frente al input de ciertos datos, el programa los relaciona con una ejecución determinada y así produce un output individualizado. El autor de la acción de manipular debe alterar este funcionamiento básico del programa y ello lo logra cuando modifica las variables, es decir, cuando modifica, reescribe o elimina ciertos datos del programa que conducen a la computadora a realizar una actividad distinta a la esperada. Un programa malicioso tiene la capacidad para alterar precisamente el flujo de datos o su integridad, lo que determina que el sistema informático sea 'engañado' en su funcionamiento y así realice vínculos irregulares entre datos almacenados (p. 324).

El mismo autor (2007) refiere que la manipulación de datos

suele presentarse en tres fases bien diferenciadas: a) La primera alternativa abarca el proceso de ingreso de datos al sistema, cuya veracidad o no resulta intrascendente para el proceso automatizado del sistema de tratamiento y almacenamiento de esos datos, pero que adquiere relevancia típica desde esta figura de estafa informática cuando esos datos, que no coinciden con la realidad, producen una alteración del resultado, provocándose así un perjuicio patrimonial indebido; b) La segunda alternativa se configura en el mismo seno del proceso de tratamiento de datos y por lo general se produce cuando el autor introduce algún virus o programa malicioso que altera el funcionamiento del sistema, provocándose con ello que los resultados derivados del tratamiento de datos sean alterados por el accionar del agente [...]; c) La tercera alternativa se manifiesta en el proceso final, es decir en el output, y ello se manifiesta cuando se altera

mediante manipulación el resultado correcto del procesamiento de datos. (pp. 324-325)

En síntesis, las notas esenciales de esta figura penal especial son la alteración del funcionamiento normal del sistema informático y/o de la transmisión de datos.

El sujeto activo puede ser cualquier persona (delito común) que tenga o no autorización para el ingreso al sistema. En consecuencia, pueden serlo tanto un empleado como un tercero ajeno a la corporación que sufre el ataque informático, en los casos en que una persona jurídica padece el delito.

Por otro lado, el sujeto pasivo es aquel a quien patrimonialmente se perjudica mediante la manipulación del sistema o la transmisión de datos, pudiéndose tratarse de personas físicas, como así también de existencia ideal, como compañías financieras, bancarias, bursátiles, aseguradoras, entre otras.

En cuanto al tipo subjetivo, la doctrina sostiene que requiere dolo directo, por lo cual el autor debe conocer y querer la realización de los elementos objetivos del tipo penal en cuestión.

Por otro lado, la figura bajo análisis requiere que exista un resultado de perjuicio patrimonial, es decir, que el sujeto pasivo haya visto disminuido su patrimonio en términos económicos por arte de la acción delictiva. La figura receptada por el art. 173, inc. 16, del CP, se consuma al momento en que se efectiviza el perjuicio económico como consecuencia de la maniobra informática llevada a cabo. No interesa aquí si el autor o los autores lograron efectivamente disponer del dinero defraudado, sino únicamente si se verificó una disminución patrimonial en los estados contables de la víctima.

En conclusión, para distinguir la aplicación de la figura bajo análisis de aquella estafa general regulada en el art. 172 del CP y/o de algún otro supuesto especial de los

regulados en el art. 173 de ese cuerpo normativo, debe verificarse la alteración del funcionamiento de algún sistema informático o de la transmisión de datos. Es decir, concretamente, establecer si los autores para acceder al sistema o a la base de datos de la víctima llevaron a cabo alguna manipulación de tipo informática que haya perturbado el correcto desenvolvimiento de algún sistema o de la propia transmisión de datos.

Por último, cabe mencionar que el delito de estafa informática (173, inc. 16, del CP) puede concurrir de forma ideal (art. 54 del CP) con el delito de daño simple o calificado (art. 183, segundo párrafo, o 184, inc. 5° o 6°, del CP), pues el acceso clandestino al sistema informático o a la base de datos del damnificado puede ocasionar la alteración, destrucción o inutilización de documentos, programas y/o sistemas informáticos. A su vez, vale aclarar que, si bien en la mayoría de los casos también se verifican los extremos típicos de la conducta delictiva prevista en el art. 153 bis del CP, lo cierto es que por razones de especialidad y gravedad esta figura queda absorbida y desplazada por aquella bajo análisis en el presente acápite.

IV. Distintas técnicas de obtención de datos sensibles y engaños informáticos

El contexto social generado con motivo del virus COVID-19 ha servido de escenario propicio para la proliferación de engaños informáticos, que se han convertido en el "cuento del tío" de la actualidad. El encierro de las personas fue un facilitador del aumento de la frecuencia consumativa al incrementarse geométricamente la utilización de las herramientas informáticas.

Entre las múltiples modalidades o técnicas utilizadas para defraudar telemáticamente a las personas —subsumibles, según el caso, en las previstas del artículo 172 o sus modalidades especiales de los incisos 15 o 16 del art. 173 del Código Penal—, cabe resaltar las siguientes:

a) Phishing*:* la palabra (del término inglés *fishing*, que significa "pescar") se refiere a la actividad por la cual mediante subterfugios técnicos o ingeniería social se intenta obtener las claves de acceso de las cuentas bancarias, los datos de las tarjetas de compra, débito o crédito u otra información sensible de una persona como rédito individual del criminal o con la finalidad de conseguir ulteriormente un beneficio patrimonial[7].

Los *phishers* se valen de múltiples métodos, cuyos constante renovación y perfeccionamiento impiden hablar de un único tipo o técnica. Sin embargo, entre los mecanismos más utilizados pueden mencionarse el envío de correos electrónicos, mensajes de texto o chats por redes sociales mediante los cuales, de forma sofisticada y bajo la apariencia de ser determinada persona o compañía, se comunica al destinatario, por ejemplo, que ha obtenido algún beneficio en la entidad financiera de la que es cliente; que es necesario la renovación de sus claves de acceso por cuestiones de seguridad; o que debe realizar algún tipo de trámite que exige, claro está, el suministro de información confidencial.

En efecto, para convencer a sus víctimas y disimular su verdadera identidad, los *phishers* utilizan nombres de dominio similares a los de las entidades financieras o reconocidos sitios de compra *online* y adoptan plataformas, logotipos e imágenes de identificación iguales a las utilizadas por dichas corporaciones. Mediante esa simulación solicitan al receptor del mensaje que proporcione datos sensibles (identificaciones, claves de acceso, códigos de tarjetas de crédito, débito o compra, etc.) o que ingrese a un enlace que lo redirecciona a una página web falsa, desde la cual se le exige

[7] El rédito no siempre se vincula con una posterior defraudación, pues en algunas ocasiones los datos obtenidos son comercializados por los *phishers* a través de la *Dark Web* u obtenidos como mera demostración de habilidades técnicas.

nuevamente el suministro de dicha información como exigencia para alcanzar el beneficio prometido o llevar a cabo algún trámite.

Las ventajas de esta clase de engaños son numerosas, pero se destacan las siguientes: la posibilidad de contactarse indiscriminadamente y de manera anónima con múltiples víctimas a la espera de que alguna de ellas "muerda el anzuelo"; la dificultad para la investigación al valorar las limitaciones en infraestructura técnica por parte de los operadores jurídicos y las habilidades de los autores para ocultar sus movimientos en la red (p. ej., utilización de programas del tipo TOR[8]); la reticencia u obstáculos burocráticos en la entrega de información por parte de empresas extranjeras privadas (p. ej. Google, Microsoft, Facebook o Twitter); la falta de herramientas procesales para pesquisar esta clase de hechos que poco tienen que ver con los delitos clásicos; y los inconvenientes que se presentan respecto de la competencia jurisdiccional para investigarlos en algunas jurisdicciones[9].

Cabe resaltar que quien se vale de *phishing* para captar datos confidenciales suele posteriormente utilizarlos para cometer alguna de las defraudaciones penadas en los incisos 15 y 16 del art. 173 del Código Penal.

Sin embargo, no menos cierto es que la mera captación de los datos, en principio, no constituiría —al menos, al tiempo de la redacción del presente artículo— delito alguno pues, respecto de las defraudaciones aquí analizadas, solo puede ser

[8] Los sistemas de este tipo (*The Onion Router*) implican una red de comunicaciones donde no es posible determinar la identidad de los usuarios que intercambian contenido.

[9] Además de los problemas para determinar el lugar de comisión del hecho (generalmente resueltos en función del principio de ubicuidad recogido por la Corte Suprema de Justicia de la Nación), en el ámbito de CABA existe una puja entre la Justicia Penal, Contravencional y de Faltas local y el Fuero Criminal y Correccional Nacional sobre quien resulta competente para investigar esta clase de defraudaciones. Véase apartado "V" de este trabajo.

entendida como un acto preparatorio no punible, dado que el uso de la información conseguida será posterior e incluso eventual[10].

No obstante, las excepciones se presentan en los casos donde se comprueba la existencia de una asociación ilícita dedicada a dichos fines en los términos del artículo 210 del Código Penal; que la obtención de los datos, mediante alguna de las múltiples técnicas de *phishing*, ha ocasionado un daño sobre el dispositivo (*hardware*) o sistema informático (*software*) de la víctima, en cuyo caso resultaría de aplicación el tipo previsto en el artículo 183, segundo párrafo y sus agravantes del cuerpo normativo citado (p. ej., cuando los datos se obtienen mediante la implantación de un virus informático); o que ha importado el acceso no autorizado a un sistema de acceso restringido (art. 153 bis del CP).

En cualquier caso, así como comprar veneno para asesinar a un enemigo no supera el umbral de la punibilidad, lo mismo ocurre —salvo las excepciones mencionadas— con la persona que obtiene subrepticiamente datos sensibles mediante alguna de las técnicas de *phishing*, circunstancia que cuanto menos evidencia la necesidad de un profundo debate legislativo respecto de la protección penal de datos personales.

A propósito de ello, en el Anteproyecto de reforma del Código Penal presentado a consideración del Congreso de la Nación en el año 2019, se incorporó un título dedicado a los "Delitos informáticos", cuyo artículo 491 reza

> Se impondrá prisión de seis (6) meses a dos (2) años o seis (6) meses a veinticuatro (24) días multas, al que ilegítimamente con ánimo de lucro o la

[10] Sin embargo, la sola utilización de dichas claves para acceder a un sistema de datos de acceso restringido sin la autorización de su titular configuraría el tipo penal previsto en el art. 153 bis del CP. Por otra parte, en el ámbito de CABA, se prevé como contravención la suplantación digital de una persona (art. 71 *quinquies* y ss. del Código Penal, Contravencional y de Faltas de la ciudad).

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.

Por otro lado, corresponde traer a colación lo expuesto en los apartados anteriores respecto de las defraudaciones previstas en los artículos 173, incisos 15 y 16 del CP, en los casos en que los datos de la víctima son captados mediante alguna técnica de *phishing*.

Así, en el caso en que la disposición patrimonial resulte consecuencia de la utilización no autorizada de los datos de las tarjetas de crédito, débito o compra, la subsunción legal que correspondería aplicar es la del inciso 15 del art. 173 del Código Penal, pues el tenor literal del precepto remite específicamente a las operaciones efectuadas ilegítimamente mediante el uso no consentido de tales instrumentos de pago o de sus datos, aunque lo fuera por medio de una operación automática.

Por otra parte, los movimientos de dinero no autorizados desde la cuenta bancaria de una persona (es decir, el *online* o *home banking*), previa obtención mediante *phishing* de sus claves de acceso —de suyo, distintas a las de las tarjetas enunciadas en el inciso 15, del art. 173 del CP—, tanto la doctrina como la jurisprudencia suelen subsumirlos en el tipo previsto en el inciso 16 del artículo citado.

En tal sentido, se considera que la "manipulación informática" se configura a partir del acceso indebido por parte del criminal en la banca virtual de un tercero con el consecuente desplazamiento patrimonial perjudicial a partir del ingreso ilegítimo de

datos (p. ej., transferencias de dinero no consentidas, solicitud de préstamos dinerarios, compra de moneda extranjera, etc.), extremo que constituye un funcionamiento anómalo y contrario del que llevaría a cabo el titular de la cuenta.

Esta interpretación supone un concepto amplio de "manipulación informática", que incluye cualquier intervención en el sistema informático consistente en alterar, modificar y/o ocultar datos, que genere un funcionamiento indebido o incorrecto de un sistema de procesamiento electrónico.

Así, por ejemplo, se ha expedido la Sala VII de la Cámara Nacional de Apelaciones en lo Criminal y Correccional en la causa número 58028/19, oportunidad en la que confirmó el procesamiento con esta calificación de quien recibió en su cuenta bancaria dinero que provenía de otra a la que se había accedido ilegítimamente mediante el uso no autorizado de sus datos y desde la que se solicitó un préstamo de dinero que, tras su acreditación, fue inmediatamente transferido a la cuenta del autor de la maniobra.

En tal sentido se sostuvo que

> En efecto […] el desarrollo de una defraudación informática no se reduce, como parece pretender la defensa, al momento de la concreta manipulación de los datos informáticos, en tanto supone la obtención de éstos, el acceso a la plataforma digital y, claro está, la posterior concreción del perjuicio patrimonial, tramo éste en el que —como se dijo— se ha verificado la intervención del imputado.

Similar postura fue adoptada por la Sala III de la Cámara Federal de Casación Penal en un caso donde se confirmó la condena de quien mediante técnicas de

manipulación informática ingresó ilegítimamente a una cuenta de *home banking* ajena y transfirió dinero a la cuenta de un tercero para retirarlo con posterioridad[11].

Más allá del criterio expuesto, otra interpretación posible es aquella que afirma que el ingreso en el *home banking* de la víctima, previa captación de datos y consecuentes desplazamientos de dinero no consentidos, no configura, en rigor, una "manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos", pues se trata de un mero uso incorrecto —o, en cualquier caso, no autorizado por parte el titular— sin que implique el funcionamiento anómalo del *software* que exige el tipo en cuestión. La laguna de punibilidad que estos hechos importarían, en atención a que el *online banking* no implica la utilización de una tarjeta de débito, crédito o compra, una omisión no justificada del legislador sin que la interpretación amplia del concepto "manipulación informática" permita una solución viable en términos jurídicos, pues constituye —según los partidarios de esta tesitura— una violación al principio de legalidad por interpretación extensiva in *malam partem* del precepto en cuestión.

Finalmente, a fin de resaltar la gravedad del asunto, en función de la numerosa cantidad de víctimas que han sufrido alguno de los tipos de *phishing*, recientemente el Banco Central de la Nación ordenó a las entidades financieras intensificar los controles de verificación de identidad de los usuarios que soliciten préstamos preaprobados[12]. A propósito de ello, algunos Tribunales han hecho lugar a medidas de no innovar requeridas por los querellantes o víctimas de las maniobras, quienes solicitan se

[11] Ver causa número 51772/11del 16 de junio de 2016.

[12] https://tn.com.ar/economia/2021/07/01/fraude-bancario-el-banco-central-impuso-mas-controles-sobre-los-creditos-preaprobados/. En igual sentido https://tn.com.ar/tecno/internet/2021/07/03/estafas-bancarias-los-nuevos-controles-del-banco-central-y-claves-para-no-ser-victimas-de-los-ciberdelincuentes

suspendan las liquidaciones de préstamo personales que fueron solicitados sin su autorización desde su *online banking* previa captación subrepticia de sus datos[13].

b) Pharming: El *pharming*[14] se trata de una técnica informática utilizada para obtener subrepticiamente información sensible de una persona, generalmente de tipo financiera o bancaria. Sin embargo, a diferencia del *phishing,* esta especial clase de engaño resulta más difícil de advertir, en tanto supone la implantación en el ordenador de la víctima de un virus o *malware* destinado a manipular las direcciones DNS —*Domaine Name Server*— que el usuario utiliza para navegar por Internet.

De esa manera, instalado el *software* malicioso en el ordenador de la víctima, esta es redireccionada a una página web falsa, generalmente idéntica a la que pretendía acceder, pero que, en realidad, es controlada por el *pharmer,* quien le extrae los códigos o claves secretas para ulteriormente cometer algún tipo de fraude.

Dado que esta técnica generalmente importa, a partir de la instalación de *software* malicioso o la modificación del *host* o *caches* en el ordenador de la víctima, la alteración del normal funcionamiento de un sistema informático o la transmisión de datos, la defraudación que ulteriormente se lleve cabo —por ejemplo, mediante transferencias de dinero o solicitudes de préstamos no consentidas desde la cuenta bancaria captada— configura sin duda alguna el tipo previsto en el artículo 173, inciso 16, del CP.

Así lo ha entendido la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal en un caso donde mediante técnica de manipulación informática —con la mención del *pharming* como una de ellas— se

[13] Así lo resolvió la Sala VII de la Cámara Nacional de Apelaciones en lo Criminal y Correccional en la causa número 44956/2020-1, "N.N.s/estafa", del 15 de marzo de 2021. En el mismo sentido la Sala IV de la Cámara citada en la causa número 14.255/21, "Klein, Elena", del 10 de mayo de 2021.
[14] El término resulta de la combinación de las palabras *farm* (la voz inglesa para "granja") y *phishing*.

ingresó a la cuenta bancaria de una persona y se solicitó un préstamo dinerario, cuyo monto fue posteriormente transferido a la cuenta de un tercero[15]. En dicha ocasión, el Tribunal sostuvo que

> Esta figura perpetrada a través de la utilización ilegítima de datos para acceder a los fondos de la víctima y efectuar transferencias a terceros produciendo el detrimento patrimonial, puede adoptar diferentes modalidades tales como la alteración de los registros, mediante correo electrónico y duplicación de sitios web comúnmente conocido como phishing, suplantando los nombres de dominio (DNS) en el ordenador de la víctima —pharming— o incluso con falsas ofertas laborales con el propósito de utilizar las cuentas bancarias de los postulantes para desviar el dinero y poder 'blanquearlo'.

c) *Skimming:* El término —que proviene del inglés *skim* y alude a la lectura por encima u hojeo de lo escrito— se refiere a la actividad por la cual se extraen subrepticiamente los datos de las tarjetas de débito, crédito o compra de una persona con la intención de clonarlas o falsificarlas y ulteriormente utilizarlas para obtener beneficios económicos en perjuicio de sus titulares o de las entidades financieras emisoras.

Al igual que el *phishing,* existen distintas modalidades de *skimming,* pero las técnicas más habituales consisten en la obtención de los datos de las tarjetas bancarias de los usuarios en el momento exacto en el que estos las utilizan por medio de dispositivos técnicos especialmente diseñados para ello.

En tal sentido, los *skimmers* suelen colocar subrepticiamente un falso lector en los cajeros automáticos o terminales de pago (*posnets*) que copia la información

[15] Cfr. Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional en la causa número 41.736, "Martinelli Stickar, Marco Antonio" del 16 de marzo de 2021.

contenida en la banda magnética de la tarjeta una vez que el usuario la desliza por dichas terminales. Así, tras obtener los datos, los grupos criminales elaboran tarjetas mellizas en plásticos vírgenes que luego utilizan como instrumentos de pago o directamente comercializan. A ese mecanismo de falso lector se añade, en algunos casos, la instalación de cámaras de filmación, que permiten también la obtención de la clave "PIN" que los clientes digitan sobre el teclado del cajero automático.

Preocupados por los graves perjuicios económicos que esta clase de técnicas ocasionan, las entidades financieras ofrecen a sus clientes guías y consejos para evitar que caigan en el engaño. Así, por ejemplo, el Banco Ciudad de Buenos Aires posee en su página web un instructivo que informa detalladamente a sus clientes sobre los distintos tipos de fraude —entre los que se incluyen el *skimming*— y las medidas que deben tomarse como protección[16].

Esta clase de actividad delictiva tiene especial relevancia —en lo que aquí interesa— en el tipo penal previsto en el art. 173, inciso 15, del CP, en tanto las tarjetas adulteradas son utilizadas para cometer la defraudación que allí se prevé. Por otra parte, cabe destacar que la sola falsificación del instrumento de pago constituye el delito previsto en el artículo 285, en función del 282 del Código Penal, y de llevarse a cabo una posterior defraudación se configuraría un concurso de delitos.

La jurisprudencia ha considerado que la mera colocación de los instrumentos destinados a copiar los datos de las tarjetas bancarias en cajeros automáticos constituye principio de ejecución de la defraudación antes mencionada, en tanto se sostuvo que

> la manipulación de cajeros electrónicos a través de la instalación de dispositivos destinados a clonar tarjetas magnéticas [lo que, de hecho, en el caso que aquí nos ocupa, se logró] revela un inequívoco propósito de defraudación —en los

[16] Ver sitio oficial del Banco Ciudad: https://www.bancociudad.com.ar

términos del art. 173, inc. 15, del C.P. — y constituye, ante la proximidad del bien jurídico con la fuente de peligro, el principio de ejecución del delito […] Así, el autor de acuerdo con su plan realizó actos que en forma inequívoca revelan un accionar que estaba dirigido a obtener datos de cuentas —los que obtuvo— los cuales usaría para comenzar la defraudación tentada reprochada.

Así, se encuentra acreditado que se encontraba en marcha el *iter criminis* de la maniobra de fraude, aun cuando la consumación —en el caso, el perjuicio patrimonial— se viera luego impedida por circunstancias ajenas a la voluntad del imputado[17].

Resta mencionar que, eventualmente, la mera tenencia de elementos o instrumentos destinados a falsificar tarjetas de crédito, débito o compra se encuentra reprimida por el artículo 299 del Código sustantivo.

d) Otras modalidades: a las modalidades engañosas enumeradas se han agregado otras que han suscitado interés público y acaparado las noticias periodísticas en materia de ciberfraudes[18], entre ellas: el *vishing*, el *smishing* y las estafas mediante transferencias por el sistema DEBIN (débito inmediato).

Las primeras dos modalidades no dejan de ser variantes del *phishing* anteriormente expuesto. Por un lado, el *vishing* —cuyo término es una combinación entre las palabras inglesas *voice* y *phishing*— alude a la técnica por la cual el autor se comunica telefónicamente con la víctima o por mensaje de voz, y mediante engaño obtiene datos sensibles; y, por otro, el *smishing* que tiene como finalidad el mismo

[17]Causa número 37747/18, "Hemmingsen, Niklas Paw Siemsem", del 14 de septiembre de 2018, del registro de la Sala V de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal.

[18] Una muestra de ello puede verse en el siguiente enlace: https://tn.com.ar/economia/2021/08/22/estafas-virtuales-una-por-una-cuales-fueron-las-mas-habituales-en-los-ultimos-meses-y-como-estar-prevenido

resultado, esto es la obtención de datos confidenciales de la víctima, pero a través del intercambio de mensajes de texto con esta (SMS).

Por último, la implementación del sistema DEBIN —débito inmediato— por parte del Banco Central sin una adecuada campaña de información ni sistema de doble verificación ha ocasionado que distintas personas hayan sido engañadas al recibir virtualmente solicitudes de "autorización de débito" que aceptan sin mayores precauciones. Es que a diferencia de las tradicionales transferencias de dinero por *home banking*, la operatoria mediante DEBIN invierte los roles de quienes interactúen, pues uno de los usuarios envía un pedido de transferencia de dinero a otra persona por un determinado monto y si esta al recibir la solicitud la acepta, se concreta inmediatamente el traspaso.

A modo de ejemplo: Juan se comunica con un local de indumentaria y tras consultarle al vendedor Pedro sobre los precios le informa que le realizará una gran compra de mercadería a pagar por transferencia bancaria. Juan le indica que su banco exige una autorización previa por parte del vendedor —engaño— y le envía la solicitud de DEBIN a Pedro, quien la acepta, consumándose así la disposición patrimonial perjudicial. Cabe destacar que esta clase de engaños constituyen una estafa en los términos del artículo 172 del Código Penal en tanto no se verifican los presupuestos típicos especiales de ninguna de las defraudaciones desarrolladas en este artículo.

V. Discusión acerca de la competencia material de las figuras bajo análisis

Los conflictos de competencia por los delitos en estudio, suscitadas recientemente entre la Justicia Nacional en lo Criminal y Correccional y la Justicia Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, han arrojado controvertidos decisorios.

El 31/03/2021, el Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires admitió la competencia de ese fuero[19] entendiendo que le correspondía la investigación y juzgamiento de delitos creados con posterioridad a la sanción de la Ley n.º 24588[20], conocida como "Ley Cafiero".

En virtud de ello, y de lo normado por el artículo 129 de la Constitución Nacional —entre otros—, el fiscal general del fuero local porteño instruyó a los fiscales de esa jurisdicción para que asuman la competencia de los tipos penales previstos en los incisos 15 y 16 del art. 173 del Código Penal[21].

Por el contrario, distintas salas de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal[22] han coincidido en que le corresponde a su ámbito jurisdiccional el conocimiento de estos delitos. Ello, con el argumento de que los tipos penales que fueron creados con posterioridad a la sanción de la ley nro. 24588 serían de atribución exclusiva y originaria del Poder Judicial de la Nación, con asiento en la Capital Federal. En efecto, la mentada ley estableció una metodología en el proceso de traspaso gradual de competencias ordinarias al fuero local, por la cual el conocimiento de cada delito debe estar expresamente incluido en los convenios que suscriban el Gobierno Nacional y el de la Ciudad Autónoma de Buenos Aires para que la justicia local resulte competente, sin que se haya incluido, hasta el momento, la transferencia de las figuras previstas por artículo 173, inc. 15 y 16 del Código Penal[23].

---

[19] Del registro del TSJ de CABA, causa número 17891-20, "NN, NN s/ presunta comisión de delito (art. 173 inc. 16 CP) s/ conflicto de competencia".

[20] Publicada en el Boletín Oficial el 30 de noviembre de 1995.

[21] Cfr. Resolución FG Nº 48/21.

[22] Sala I, "Berenguer, M. V. s/competencia" (Causa Nº 36.258/2020) del 13/10/2020; Sala VII, "N.N. s/competencia, defraudación manipulación informática" (Causa Nº 17.507/2021) del 11/06/2021; y Sala V, "Todorov, I. s/estafa" (Causa Nº 12.274/2019) del 16/06/2021, entre otras.

[23] Las defraudaciones previstas en los incisos 15 y 16 del art. 173 del Código Penal no fueron incluidas en las leyes 25272, 26357 y 26702 que dispusieron la transferencia de determinados delitos al ámbito de conocimiento de la justicia de la Ciudad Autónoma de Buenos Aires. Siquiera podría adquirir operatividad lo dispuesto en el artículo 2 de la mencionada ley 26702 (Boletín Oficial del 6-10- 2011),

Del mismo modo, se hizo hincapié en el precedente "Zanni" de la Corte Suprema de Justicia de la Nación, donde se sostuvo que

> no resulta admisible considerar inserta dentro de la competencia local a cada conducta ilícita que, con posterioridad a la ley 24.588, sea catalogada como delito en el sentido señalado por el juez correccional en su resolución sino que, contrariamente, los nuevos tipos penales que, eventualmente se sancionen en el futuro, a menos que contengan disposiciones expresas, deben ser sometidos a un nuevo convenio de partes y posterior ratificación legislativa, para integrar la jurisdicción local[24].

Ahora bien, más allá de la posición que se tome respecto de la interpretación que se les asigne a las leyes mediante las que se acordó el traspaso de ciertos delitos, entendemos que también deben tenerse en cuenta otros parámetros para determinar la competencia de las conductas en trato, los que fueron expuestos en forma clara por el juez Pinto —y a los que adherimos— al momento de expedirse en una de las primigenias contiendas[25].

En la ocasión sostuvo que

> Los elementos objetivos que prevé el tipo penal permiten avizorar que los hechos donde tales conductas tienen lugar exceden posiblemente el interés local, en tanto potencial afectación a otras jurisdicciones. Sólo a modo ilustrativo, es posible reconocer que dichas modalidades delictivas suelen involucrar a autores y partícipes que efectúan aportes desde distintos lugares respecto a donde la

---

que reza "Asígnese al Poder Judicial de la Ciudad Autónoma de Buenos Aires la competencia para investigar y juzgar los nuevos delitos de competencia penal ordinaria, aplicables en su ámbito territorial, que se establezcan en lo sucesivo en toda ley de la Nación, salvo que expresamente se disponga lo contrario", al regir ambos tipos penales con anterioridad a la ley 26702.

[24] Fallos 333:589.

[25] Cfr. Sala V de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, causa n° 26.896/20, "Pries, Enrique", del 28/8/20.

víctima se encuentra. Asimismo, también los alcances del perjuicio económico pueden trascender de la jurisdicción de la Ciudad Autónoma de Buenos Aires, y además suelen traducirse en la existencia de varias jurisdicciones investigando la misma maniobra. Los avances tecnológicos en este sentido han traído aparejados nuevas modalidades delictivas que amenazan las ideas tradicionales relativas a los límites de competencia en tal sentido y exigen un abordaje integral para lograr una respuesta correcta a la sociedad (véase a modo de ejemplo las maniobras conocidas como *phishing*, *pharming*, *hacking* y *cracking*).

Sentado ello, cabe destacar que los fiscales generales a cargo de las fiscalías n.° 1, 2 y 3 ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, pusieron en conocimiento del procurador general la Nación las numerosas contiendas de competencia suscitadas con la justicia local a partir del referido precedente del Tribunal Supremo de la CABA y de la instrucción general dictada por el procurador del Ministerio Público Fiscal del mismo ámbito local, como así también la decisión adoptada por estos de sostener la competencia de ese fuero para intervenir en los casos abarcados por los tipos penales bajo examen, brindando los fundamentos que abonaban esa postura.

Ello derivó en que el Dr. Casal, en su carácter de procurador General de la Nación, emitiera recientemente[26] una resolución dirigida a todos los fiscales en torno al asunto, ocasión en la que coincidió con la posición de los fiscales de cámara, que se encontraba alineada con el mentado fallo "Zanni". Al respecto, opinó que los tipos penales bajo estudio no podían entenderse como nuevos delitos, sino que se trataba de distintas modalidades de defraudación, las que se encontraban previstas desde la sanción del Código Penal en 1921. Además, aclaró que la incorporación de los incisos 15 y 16 al

[26] Conf. Resolución PGN 38/22 del 6/6/22.

artículo 173 se realizó en los años 2004 y 2008, respectivamente, es decir, con anterioridad a la sanción de la referida ley.

Bajo tales premisas, a los fines de unificar el criterio de actuación, concluyó que no existiendo una norma que expresamente transfiriera la competencia en la investigación de esas conductas y el juzgamiento de los hechos ocurridos en la órbita de la Ciudad de Buenos Aires, que se subsumieran bajo las previsiones legales mencionadas, no integraban la competencia de los tribunales locales.

A pesar de ello, tendremos que aguardar el temperamento que tomará al respecto la Corte de Suprema de Justicia de la Nación, que deberá zanjar finalmente la cuestión.

VII. Conclusiones

El paso del tiempo ha demostrado que la propuesta de incorporación al Código Penal de conductas vinculadas a la comisión de delitos informáticos, efectuada en el mentado VI Congreso Latinoamericano de 1998, era adecuada y certera. No solo porque este accionar delictivo se ha consagrado como una nueva forma de criminalidad, sino también porque algunas de las referidas propuestas han coincidido con las modificaciones legislativas que se llevaron a cabo.

En lo que aquí interesa, la proposición respecto de la adecuación del Capítulo IV sobre "Estafas y otras defraudaciones" ha tenido correlato en el dictado de las leyes 25930, de fecha 21 de septiembre de 2004, y 26388, del 25 de junio de 2008, a través de las cuales se tipificaron las defraudaciones vinculadas directamente con las tarjetas de compra, crédito o débito, con los datos personales de sus tenedores y con las técnicas de obtención de información vía telemática.

El inciso 15 del artículo 173 del Código Penal protege el patrimonio de las personas a través de la penalización de la utilización fraudulenta de las tarjetas de

compra, crédito o débito siempre y cuando hubieran sido falsificadas, adulteradas, hurtadas, robadas, perdidas u obtenidas del legítimo emisor mediante ardid o engaño o mediante el uso no autorizado de sus datos, de esta manera se evita la manipulación ilegal o irregular de una tarjeta o de sus datos en operaciones automatizadas.

Complementando la protección digital patrimonial se destaca el inciso 16 del artículo 173 del Código Penal, en el cual se tipifica la defraudación a través de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o transmisión de datos. De esta manera, con la redacción actual resulta de modalidad abierta pudiendo utilizar el autor del delito cualquier técnica de manipulación informática, es decir, cualquier modificación del proceso de datos, lo que la diferencia del tipo básico de estafa que requiere el error de la persona.

En ese sentido, resulta pertinente aclarar que serán las circunstancias fácticas del caso las que determinen la subsunción de la conducta bajo la modalidad de defraudación que corresponda, ya que debe tenerse en cuenta que aun cuando las estafas involucren medios telemáticos en su comisión, no necesariamente tendrán adecuación típica en los términos de los incisos 15 y 16 del artículo 173 del Código Penal, sino que podrán configurar el tipo penal previsto por el artículo 172. Tal puede ser el caso de la persona que dolosamente ofrece un producto a la venta en la web, y tras venderlo recibe el pago, pero no lo entrega.

Asimismo, también se detallaron los supuestos de obtención ilegal de datos, es decir, el *phishing, pharming, skimming*, entre las técnicas más destacadas. En relación con el punto, queremos poner énfasis en que el pilar fundamental para no convertirnos en víctimas de estas artimañas es la prevención que descansa en los recaudos que debemos tomar para mantener incólumes nuestros datos personales.

Así, entendemos que las entidades bancarias o cualquier plataforma a través de las que se opere en forma digital tienen la obligación no solo de realizar campañas de información y prevención, sino también de tomar medidas de acción tendientes a asegurar la efectiva identidad del cliente al momento de realizar una operación comercial.

En tal sentido, celebramos que el Banco Central de la República Argentina haya instado a las entidades financieras con el objeto de que en las solicitudes de acreditación de créditos preaprobados a través de canales electrónicos se verifique fehacientemente la identidad del peticionante, lo que deberá realizarse mediante técnicas de identificación positiva, tales como controles biométricos o de acceso a través de una comunicación electrónica o telefónica.

Desde nuestra parte, aconsejamos evitar brindar información personal; contactarse con cuentas oficiales cotejando que estén verificadas; no suministrar contraseñas de ningún tipo, tales como de *home banking*, token, usuarios digitales, tarjetas de compra, débito o crédito; establecer contraseñas complejas con caracteres especiales, números, mayúsculas; realizar la verificación en dos pasos para asegurar la identidad del titular de redes sociales o teléfonos celulares; no utilizar la misma clave para todas las plataformas con las que se operen; no ingresar datos personales en sitios utilizando enlaces que llegan por correo electrónico; y no atender llamadas telefónicas de entidades financieras, ante ello, recomendamos al usuario que directamente establezca la comunicación.

Por último, a pesar de lamentar las numerosas y crecientes denuncias en la materia, consideramos que, a la postre, esta experiencia servirá para mesurar y mejorar la eficacia de las técnicas de investigación y de las herramientas disponibles para el combate de este tipo de delincuencia tan compleja que ha llegado para quedarse.

Referencias bibliográficas

ABOSO, G. (2007). *Cibercriminalidad y derecho penal*, 1ra edición. Buenos Aires. Ed. B de F.

LEVENE, R. (nieto) y CHIARAVALLOTI, A. (1998). Delitos Informáticos, en *Revista La Ley -nro. 202-*. Buenos Aires: La Ley.

PALAZZI, P. (2009). *Los Delitos informáticos en el Código Penal. Análisis de la ley 26.388*. Buenos Aires: Ed. Abeledo Perrot.

PASTOR MUÑOZ, N. (2006). Parte especial, en Jesús-María Silva Sánchez (Dir.), *Lecciones de derecho Penal*. Barcelona: Ed. Atelier.

Apartado normativo

Código Penal.

Constitución Nacional.

Convenio de Budapest (sobre ciberdelincuencia).

Ley 24588.

Ley 25065.

Ley 25930.

Ley 26388.

Ley 26.92.

Apartado de jurisprudencia

"Berenguer, M. V. s/competencia"

"Hemmingsen, Niklas Paw Siemsem"

"Klein, Elena"

“Martinelli Stickar, Marco Antonio”

“N.N. s/ estafa”

“N.N. s/ presunta comisión de delito”

“Pries, Enrique”

“Todorov, I. s/ estafa”

“Zanni”