Departamento de Derecho

Maestría en Derecho Penal

Actividad delictiva en un mundo ciber conectado.

Defraudación mediante el empleo de phishing: Análisis dogmático, dificultades en su investigación, y necesidad de reforma legislativa.

Alumno: Facundo J. Alvaredo (DNI 35.317.594)

Tutor: LL.M. Jonathan Polansky

Ciudad Autónoma de Buenos Aires, 21 de octubre del 2024

ÍNDICE TEMÁTICO.

Resumen:

En el presente trabajo, se busca realizar un aporte que permita establecer una serie de criterios rectores que posibiliten interpretar jurídicamente la tipicidad de una conducta cuando, a través de la maniobra conocida como *phishing*, se ocasiona un perjuicio patrimonial a un tercero. En dicha línea, a su vez, se esbozará un análisis dogmático de dicha maniobra y se la intentará vincular con algunos de los tipos penales existentes en nuestro derecho sustantivo.

También, en el desarrollo, se intentará ilustrar la importancia que reviste la circunstancia de contar con tipos penales específicos que contengan a la totalidad de las maniobras que comprenden al *phishing*. Todo lo anterior, a su vez, realizando una correcta tarea en lo referente a contemplar las dificultades que esta maniobra presenta en materia de investigación, circunscribiéndonos al caso concreto de lo que sucede en el territorio de la Ciudad Autónoma de Buenos Aires.

Por último, se intentará demostrar, a través de la legislación comparada y la historia reciente, diferentes técnicas legislativas que han logrado receptar a esta modalidad delictiva fraudulenta.

I. Introducción.

El *phishing* es una *"*maniobra tendiente a la obtención de información confidencial de terceros, mediante técnicas de ingeniería social que involucran correos electrónicos, sitios web o perfiles en redes sociales engañosos, en los que los autores se hacen pasar por terceros"[1].

Se ha dicho que el *phishing* opera como antesala para la comisión de ciertos delitos[2] debido a que, cuando se lo analiza en el plano del *iter criminis* según el tipo penal del que se trate, se puede apreciar que se suele ubicar en el segmento de los actos preparatorios o del comienzo de ejecución. Esto dependerá del plan específico del autor, y será estudiado en el transcurso de este trabajo.

Concretamente, se estudiará una maniobra defraudatoria que resulta ser la que mayor cantidad de reportes y denuncias recibe en la actualidad en nuestro país[3]. Se trata de una modalidad delictiva mediante la cual, a través del *phishing*, los autores -*phishers*- buscan obtener datos personales informáticos de sus víctimas -en particular vinculados a usuarios y claves de cuentas bancarias y plataformas de pago y gestión de dinero- para obtener una ventaja patrimonial.

Es así que el autor del hecho debe, de alguna forma, violar la privacidad y la confidencialidad de las bases de datos para acceder a la información personal de carácter identificatorio que posea la víctima. Con posterioridad, en algunos casos y en virtud de la situación ventajosa en la que se ha colocado el autor respecto del patrimonio de la víctima al haber obtenido sus datos y claves personales, éste puede lesionar su patrimonio al acceder a los datos vinculados con la entidad (frecuentemente bancaria, pero también puede ser comercial) que se trate[4]. Es decir, se trata de una maniobra defraudatoria que los autores de esta clase de hechos llevan a cabo a través del empleo de *phishing*.

De tal modo, se estudiará si la conducta descripta en los párrafos precedentes se encuentra receptada por alguno de los tipos penales contenidos en nuestro ordenamiento jurídico (por ejemplo: arts. 172, 173 inc. 16°, y 162); o si, por el contrario, se torna necesario discutir una eventual reforma legislativa que contenga al *phishing* en el marco

[1] UFECI – Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Buenos Aires, 2021. Pág. 14.
[2] ROIBÓN, María M. "Reflexiones sobre el acceso ilegítimo a un sistema o dato informático". En Revista Erreius, "Cibercrimen y Delitos informáticos". Buenos Aires, 2018. Págs. 137-138.
[3] UFECI – Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Buenos Aires, 2021. Pág. 18.
[4] Ibidem.

de una defraudación patrimonial: al cual, en adelante, nos referiremos generalmente como *phishing defraudatorio*.

Se trata de una conducta compleja que afecta, principalmente, la privacidad y la propiedad como bienes jurídicos penalmente protegidos[5].

Ahora bien, y a fin de continuar con el marco introductorio, se torna necesario señalar a partir de qué momento histórico comenzó el interés por parte de los Estados Nacionales de definir, precisar, investigar y perseguir aquellas conductas delictivas que tienen lugar en el ciberespacio: con las cuales el *phishing* mantiene una relación de especificidad. Varias de las cuales, posteriormente, encontrarían acogida en diversos tipos penales creados a tal efecto, convirtiéndose así en ciberdelitos.

Lo anterior ocurrió en el año 2001, cuando el Consejo de Europa impulsó la creación del Convenio de Budapest sobre Ciberdelincuencia. Éste fue un tratado internacional creado con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet[6]. Lo anterior, amén de la necesidad de aplicar, con carácter prioritario, una política penal común con el objetivo de proteger a la sociedad frente a la ciberdelincuencia. En particular, mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

En ese marco, y a través de dicho Convenio, se encomendó a los estados parte la tipificación de una serie de delitos considerados como habituales en la ciberdelincuencia. Ejemplos de esto son los arts. 7 y 9 de la norma citada que refieren a la "Falsificación informática" y a "Delitos relacionados con la pornografía infantil", respectivamente.

Ahora bien, y no sin dificultades interpretativas, el art. 8 del Convenio de Budapest sobre Ciberdelincuencia, recomendó a los estados parte la tipificación del Fraude Informático[7].

En ese marco internacional, en el año 2008, Argentina promulgó la Ley 26.388 la cual, tomando como referencia lo dispuesto por la norma señalada en el párrafo precedente, creó el tipo penal de la defraudación informática que actualmente está legislado en el art. 173, inc. 16, del Código Penal Argentino[8]. A lo largo de este trabajo,

[5] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 166-167.
[6] Convenio de Budapest. Council of Europe. Serie de tratados europeos n°185. Págs. 2-3.
[7] Convenio sobre la Ciberdelincuencia. Budapest, 23.XI.2001. Consejo de Europa.
[8] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 157-158.

veremos que ese tipo penal no recepta al *phishing defraudatorio* y cuáles son las razones que fundan dicha conclusión.

También se torna imperioso remarcar que, a los fines prácticos, este trabajo se va a delimitar al territorio correspondiente a la Ciudad Autónoma de Buenos Aires.

Ahora bien, y a los fines de situar el contexto, a partir de la reciente pandemia experimentada a nivel mundial por COVID-19, se advirtió una creciente tendencia hacia el aumento de estas maniobras delictivas. En efecto, la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación -UFECI- ha expresado, en su informe de gestión correspondiente al año 2020, que se han cuadriplicado la cantidad de reportes relacionados con defraudaciones patrimoniales mediante el empleo de *phishing* (de 244 a 1079 casos) debido, a su vez, al incremento en la utilización de medios electrónicos.

En otro orden de ideas, no huelga destacar que estas modalidades delictivas suelen estar dirigidas a los sectores más vulnerables en lo que respecta al uso de herramientas informáticas: personas sin experiencia en su uso, sin acceso a las debidas protecciones informáticas en materia de software/antispam/firewall/etc.[9]. Todo lo cual, a su vez, redunda en el creciente temor de ese sector al uso de las herramientas digitales para llevar a cabo sus transacciones comerciales: herramientas que han demostrado ser más seguras y eficientes que el mero intercambio presencial de bienes y servicios.

En esa línea, el aumento del número de reportes vinculados a las defraudaciones mediante el empleo de *phishing* no resulta un dato meramente accidental, sino que es reflejo del fuerte aumento que el eCommerce ha experimentado en nuestro país en los últimos años. Concretamente, sumados los períodos anuales correspondientes a los ciclos 2020[10], 2021[11] y 2022[12], Argentina ha mostrado un incremento de casi cuatro (4) millones de nuevos usuarios con relación a esta modalidad de transacción comercial. A su vez, de tales estadísticas se desprende que, si bien el método de pago más elegido sigue siendo la utilización de tarjetas de crédito y/o débito, el empleo de billeteras electrónicas ha crecido hasta ubicarse en el puesto nro. 4, actualmente[13]. Por otra parte, la mayoría de los usuarios realiza dichas transacciones desde su *smartphone*. Todo lo cual, nos lleva a asumir el

[9] TEMPERINI, Marcelo. "Delitos informáticas y cibercrimen: alcances, conceptos y características". En suplemento especial, Erreius. Buenos Aires 2018. Pág. 64.
[10] CACE – Cámara Argentina de Comercio Electrónico. Informe anual de comercio electrónico 2020.
[11] CACE – Cámara Argentina de Comercio Electrónico. Informe anual de comercio electrónico 2021.
[12] CACE – Cámara Argentina de Comercio Electrónico. Informe anual de comercio electrónico 2022.
[13] CACE – Cámara Argentina de Comercio Electrónico. Informe Mid-term 2024.

exponencial crecimiento que han visto, no sólo los medios informáticos respecto de estas transacciones comerciales, sino de usuarios que cada vez más eligen estas nuevas modalidades.

Asimismo, a nivel mundial, casi el 60% de las empresas han manifestado que su principal preocupación es "…la posibilidad de un ataque informático de tipo *phishing" (sic)*[14]. Este dato refiere, precisamente, al principio que afirma que el usuario es el eslabón más débil de todo sistema informático y es, precisamente, el usuario quien está más expuesto a dichos ataques[15]. En particular, aquellos que pertenecen al grupo social señalado como vulnerable.

Volviendo al eje de esta trabajo, ya hemos establecido que el *phishing* es la antesala a la comisión diversos tipos penales ¿Y a cuáles concretamente? Veamos.

En primer lugar, cuando la *pesca* de datos es utilizada para ingresar a las cuentas/datos del sujeto pasivo, sin afectar su patrimonio, estaremos ante la figura tipificada en el art. 153bis del Código Penal.

En segundo lugar, si el *phishing* es empleado para modificar, destruir y/o inutilizar documentos, programas o sistemas informáticos, entonces, estaremos ante la figura legislada en el art. 183, segundo párrafo, del Código Penal.

Ahora bien, señalado lo anterior, se advierte que existe la maniobra delictiva que ya fue mencionada al inicio de esta introducción. La cual, pese a ser la más reportada/denunciada en la actualidad, no encuentra arraigo firme en ninguno de los institutos legales señalados anteriormente. Nos referimos a aquellos casos en los cuales, se utiliza el *phishing* como modalidad comisiva para obtener los datos personales e informáticos de la víctima; concretamente, nombres de usuarios y claves vinculados a plataformas de *homebanking*, aplicaciones de compraventa (Ebay), gestión de compras (MercadoPago), etc. Lo anterior, con el objeto de obtener un beneficio patrimonial para sí y/o para un tercero. A los fines prácticos, vamos a señalar que éste sería un supuesto en el cual el *phishing* opera como la antesala de una conducta de índole defraudatoria, es decir: *phishing defraudatorio*.

[14] COMJIB. "Corrupción, Ciberdelito y Otros delitos medioambientales". Grupo editorial Tirant lo Blanch. España, febrero del 2023. Pág. 8.
[15] Íbidem.

Actualmente, cuando hablamos de *phishing defraudatorio*, el debate jurídico se centra en qué tipo penal dentro de nuestro ordenamiento nacional recepta mejor esta conducta[16]. En el marco de dicho debate, existen una serie de posturas.

Por un lado, se afirma que la conducta encuentra arraigo en el delito tipificado en el art. 173, inc. 16, del Código Penal, creado a raíz de la promulgación de la Ley 26.388, comúnmente conocido como "estafa informática". Esa norma establece: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos". No obstante, cuando se reportan casos de *phishing defraudatorio*, por lo general, suele no configurarse el elemento del tipo objetivo referente a *alterar el normal funcionamiento de un sistema informático o la transmisión de datos*.

Por esa razón, otro sector -no menor- de la jurisprudencia nacional se inclina por afirmar que el *phishing defraudatorio* no representa una modalidad delictiva diferente con respecto a aquellas ya contenidas en la estafa común, tipificada en el art. 172 de nuestro código de fondo[17]. Lo anterior, toda vez que, si bien ya establecimos que el *phishing* es la antesala a la comisión de este tipo de delitos; cuando hablamos de la estafa común, dicha modalidad delictiva parecería presentar similitudes con las modalidades comisivas vinculadas al tipo penal del art. 172 del código de fondo, a saber: el ardid o engaño.

Finalmente, en caso de que no nos decantemos por ninguna de las posturas reseñadas previamente, restará analizar si el *phishing defraudatorio* puede ser calificado a la luz del tipo penal del hurto simple -art. 162 del Código Penal-.

Por último, la Ley 26.702 de "Transferencia de Competencias Penales y Contravencionales de la Justicia Nacional Ordinaria a la Ciudad Autónoma de Buenos Aires" dispuso, en lo referente a "Delitos Vinculados a Competencia Pública Local", en sus incisos "c)" y "d)", el traspaso de una serie de tipos penales correspondientes a los delitos obrantes en el Capítulo IV del Título VI de nuestro código de fondo. En tal escenario, la Procuración General de la Ciudad Autónoma de Buenos Aires dispuso que deberán ser las fiscalías de ese fuero las que entenderán en aquellos casos en los que se

[16] Esta conclusión fue extraída de la lectura y análisis de una serie de fallos emanados tanto del TSJ de CABA, como de la Cámara Nacional de Apelaciones en lo Criminal y Correccional. A saber: Expte TSJ n°17.910/2020-0, Expte TSJ n°129.685/2022-0, 17.507/2021/CA1 CCC 53.269/2022, CCC 6.378/2023, CCC 61.832/2023, CCC 33.241/2022, entre otros.

[17] Esto surge del análisis de numerosos fallos emanados del Supremo Tribunal de Justicia de la Ciudad Autónoma de Buenos Aires: Expte. Nro. 17.910/2020, Expte. Nro. 120.041/2021, Expte. Nro. 172.811/2021, entre otros.

denuncie una conducta que pueda ser calificada dentro de los estándares del art. 173 inc. 16 del Código Penal, dentro del territorio de la ciudad[18]. De esto se desprende que, además de las dificultades dogmáticas que presenta el *phishing* -y, consecuentemente, el *phishing defraudatorio*- en su interpretación, hay que adicionar los problemas que se generan en torno a las cuestiones de competencia, en tanto la decisión respecto al tipo penal involucrado impacta en cuál será la jurisdicción a cargo de la investigación: la justicia de la Ciudad Autónoma de Buenos Aires (en caso que la conducta se califique como "estafa informática") o la justicia nacional (en caso de entender que el tipo penal que correspondiente es el del art. 172).

II. *Phishing*: primera aproximación.

A. Casos en los que el phishing opera como antesala para la comisión de una defraudación ¿Qué tipo penal recepta esta maniobra?

Se ha afirmado que *phishing* implica, valga la redundancia, la *pesca* de información confidencial perteneciente a terceros, mediante técnicas de ingeniería social[19].

En este sentido, identificar en qué segmento del *iter criminis* ubicaremos al *phishing* dependerá, en gran medida, del tipo penal con el cual se lo vincule y del plan del autor. Lo anterior, podría llevar a la necesidad de definir el criterio a utilizar conforme los lineamientos adoptados por la Teoría del Delito moderna. Todo lo cual excede el objeto de estudio que conforma este trabajo. Ello, sin dejar de restarle relevancia a la idea de que el *phishing*, como maniobra, suele operar como antesala para la comisión de determinados delitos -como aquellos enumerados en la introducción-.

Actualmente, nos encontramos con una serie de problemáticas en torno a esta maniobra, siendo tan solo la primera de ellas la dificultad en cuánto a dilucidar qué tipo penal la recepta.

Concretamente, y conforme surge de los recientes fallos emanados del Supremo Tribunal de Justicia de la Ciudad Autónoma de Buenos Aires -que veremos a continuación en el ítem "C"-, la mayoría de las maniobras defraudatorias mediante el

[18] Es una lectura que se desprende del fallo "Bazán" de la CSJN (CSJ N°4652/2015). Esta postura tampoco es unánime y se contrapone con lo establecido por la Procuración General de la Nación en la Resolución PGN N°38/2022.
[19] La definición precisa fue brindada al inicio de este trabajo.

empleo de *phishing* pueden encontrar arraigo en dos (2) calificaciones legales distintas: la estafa común -art. 172 del Código Penal de la Nación- y la defraudación informática -art. 173, inc. 16, del Código Penal de la Nación-.

Ambas posturas cuentan con argumentos válidos para sostener la aplicabilidad de uno u otro tipo penal, siendo que la postura mayoritaria a nivel jurisprudencial boga por la calificación asignada en el art. 172 del Código Penal de la Nación.

Por otra parte, vale la pena poner de relieve que hace algunos años existió una postura, actualmente ya descartada por los tribunales de alzada locales[20], que pretendió vincular al *phishing defraudatorio* con el hurto simple -art. 162 del Código Penal de la Nación-.

En lo que al presente trabajo respecta, analizaremos críticamente las posturas reseñadas y explicaremos por qué ninguna acaba por receptar íntegramente todos los elementos que componen a la conducta defraudatoria traída a estudio.

B. Jurisprudencia dividida.

De un análisis pormenorizado de las decisiones del Supremo Tribunal de Justicia de la Ciudad Autónoma de Buenos Aires surge que la mayoría de los reportes vinculados con maniobras defraudatorias mediante el empleo de *phishing*, en los cuales la víctima radica la denuncia dentro de la ciudad, son provisoriamente calificados como defraudaciones informáticas en los términos del art. 173, inc. 16, del Código Penal[21]. No es hasta avanzada la investigación fiscal preliminar que el reporte recibe una nueva calificación -que usualmente coincide con la consagrada en el art. 172 del Código Penal-, donde se abre la contienda de competencia[22] a fin de que el expediente sea remitido al fuero correspondiente.

Por otra parte, existe una opinión minoritaria de la jurisprudencia vinculada al fuero de la Justicia Nacional en lo Criminal y Correccional -que será analizada más adelante en este trabajo- que afirma que estas maniobras defraudatorias mediante el empleo de *phishing* deberían ser calificadas como defraudaciones informáticas[23]. Ahora

[20] Conforme surge del criterio impartido por el fallo emanado de la Cámara Nacional de Casación en lo Criminal y Correccional, en el marco de la CNCC. Causa Nro. 46.743/2017 -Reg. nro. 1190/2021-.
[21] Expte TSJ n°17.910/2020-0 caratulado "NN, NN s/ presunta comisión delito (competencia) (art. 173 inc. 16) s/ Conflicto de competencia I".
[22] Expte TSJ n°129.685/2022-0 caratulado "Incidente de competencia en autos Ortiz, Jonathan y otros sobre 173 inc. 16 – defraudación informática s/conflicto de competencia" sentencia de fecha 15 de septiembre de 2022.
[23] Cámara Nacional de Apelaciones – Sala 7. Causa nro. 17.507/2021/CA1 caratulada "NN. Dte. O.,C. Competencia. Defraudación por manipulación informática".

bien, en los últimos años, esta interpretación ha perdido relevancia en el ámbito de dicho sistema de organización de justicia en favor de la opinión contraria[24].

Esto último ha tenido una evidente consecuencia en lo que atañe a la resolución de este tipo de casos: la mayor parte de los reportes de *phishing defraudatorio* son inicialmente investigados en el seno de la justicia de la ciudad para luego ser juzgados por el fuero nacional.

C. Maniobras actuales.

Como se ha dicho, las maniobras defraudatorias mediante el empleo de *phishing* que mayormente se llevan a cabo en la actualidad son aquellas que se efectúan "mediante técnicas de ingeniería social que involucran correos electrónicos, sitios web o perfiles en redes sociales engañosos". Tales conductas implican la receptación de un correo/mensaje/enlace que dirige al sujeto pasivo a un sitio web falso que, posteriormente, conduce a la víctima a realizar un acto de disposición de datos personales – números y nombres de usuario, contraseña, etc.- que acaba por ocasionarle un perjuicio económico[25]. Todo lo cual, finalmente, conducen a un perjuicio patrimonial por parte de la víctima respecto de aquel sujeto activo que dirigió la *pesca*.

A fin de ilustrar mejor lo anterior, se van a tomar a modo de ejemplo, algunas construcciones fácticas emanadas de la justicia local.

En primer orden, en el Expediente Nro. 17.910/2020 del Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires, se investigó un suceso que tuvo lugar el 2 de octubre del 2019. En dicha oportunidad, el presunto damnificado habría recibido un llamado telefónico por parte de su hermano, quien le habría solicitado prestada su cuenta bancaria ya que "había ganado un sorteo de la empresa Samsung por haber mantenido su línea telefónica activa" y, seguidamente, recibió otro llamado de una persona que se identificó como "Franco, empleado de la firma Samsung*"* que le indicó que se dirigiera a un cajero automático para cambiar la clave de homebanking y obtener la clave *token*. Fue así que, la presunta víctima, tras obtener la clave mencionada, se la facilitó a dicha persona: tras lo cual verificó, en su cuenta bancaria, el faltante de ciento

[24] Esta conclusión se extraer de lo resuelto por la Cámara Nacional de Apelaciones en numerosos expedientes: CCC 53.269/2022, CCC 6.378/2023, CCC 61.832/2023, CCC 33.241/2022, entre otros.
[25] UFECI – Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Buenos Aires, 2021. Pág. 14.

setenta mil pesos argentinos ($170.000) que habían sido solicitados a través de un préstamo[26].

En segundo lugar, en la Causa nro. 34.255/2018 que tramitó ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional, se investigó la conducta de un grupo de individuos que, haciéndose pasar por ejecutivos de una entidad bancaria, enviaron una serie de correos electrónicos a clientes de dicha entidad a los fines de solicitarles sus datos de usuario y contraseña de homebanking alegando problemas en el servicio y en el sistema. Con posterioridad, y habiendo accedido a dicha información, los coimputados realizaron una serie de transferencias a cuentas de su propiedad. Dicha conducta fue calificada por la Cámara de Apelaciones como constitutiva del delito de defraudación mediante manipulación de un sistema informático. Éste fue uno de los primeros precedentes en los cuales, con motivo de la discusión jurisprudencial suscitada, se discutió si *phishing* era sinónimo de *hacking*: respuesta que hoy en día entendemos como negativa[27].

Por último, y este será el ejemplo que más se ajuste a la modalidad delictiva analizada en este trabajo, en la Causa nro. 60.479/2019/TO1, la Cámara Nacional de Apelaciones en lo Criminal y Correccional, se pronunció con relación a un suceso que tuvo lugar el 19 de agosto del 2019. En dicha ocasión, la víctima recibió un llamado anónimo por parte de una persona que se identificó como autoridad del banco Itaú a través de la cual le requirió actualizar los datos de su cuenta homebanking. Mediante dicha maniobra, el autor de la maniobra logró obtener los datos "token" vinculados con la cuenta homebanking de la víctima, lo que le permitió, consecuentemente, acceder a su contraseña. De esta manera, al utilizar el sujeto pasivo su tarjeta de crédito para realizar una serie de compras, notó un faltante de ciento ochenta mil ($180.000) pesos argentinos que habrían sido transferidos a la cuenta del presunto imputado. Dicha conducta fue calificada, inicialmente, por el juzgado que intervino en la instrucción de la causa, como constitutiva del delito de estafa común y; posteriormente, la Cámara Nacional de Apelaciones en lo Criminal y Correccional estableció la calificación provisoria de defraudación mediante técnicas de manipulación de un sistema informático: lo que, a su vez, motivó una posterior contienda de competencia con el fuero de la Ciudad Autónoma

[26] TSJ CABA. Expte. Nro. 17.910/2020 s/ "NN, NN s/00 – Presunta comisión de delito (competencia) (art. 173 inc. 16) s/ conflicto de competencia I".
[27] Cámara Nacional de Apelaciones en lo Criminal y Correccional. CNCC Nro. 34.255/2018, caratulada "BENTANCOUR, Yesica D. y otros s/ procesamiento".

de Buenos Aires. En este caso, la contienda de competencia se resolvió en favor del fuero nacional, y se le asignó al suceso la calificación legal provisoria de la estafa común[28].

Finalmente, y en lo que atañe exclusivamente al *phishing* como modalidad comisiva, existen definiciones que rezan lo siguiente: "Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas"[29]. Es decir, cada vez es más común encontrar interpretaciones que afirman que el alcance de dicha maniobra también encierra una ultrafinalidad, la cual puede conducir a la *suplantación de identidad*. Esta última característica es la que se puede vislumbrar de la plataforma fáctica desarrollada en el Expediente TSJ Nro. 172.811/2021 transcripta en el párrafo precedente.

III. Análisis dogmático del Art. 173 inc. 16 del Código Penal.

A. Creación del tipo penal de la defraudación informática.

El tipo penal del art. 173, inc. 16, del Código Penal fue creado a raíz de la promulgación de la Ley 26.388 en el año 2008. Para comenzar, es necesario recordar qué reza el art. 173, inc. 16, del Código Penal: "*Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: Inc. 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.*".

Para comprender la introducción de esta modificación legislativa, es menester destacar que, en el año 2001, el Consejo de Europa impulsó el Convenio de Budapest sobre Ciberdelincuencia.

En su art. 8, la mencionada Convención instó a los Estados parte a legislar el Fraude informático al redactarse la siguiente cláusula: "*Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier forma de atentado al funcionamiento de un*

[28] Cámara Nacional de Apelaciones en lo Criminal y Correccional. Causa Nro. 60.479/2019/TO1, caratulada "Narciso Yedros, Fabián s/ estafa -procesamiento-".
[29] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero" (art. 8º).

Volviendo al eje del presente trabajo, es dable entender que no es la "ausencia de autorización" lo que define al *phishing defraudatorio*. Sino la forma engañosa que caracteriza a la obtención de información -datos, claves, etc.- por parte del sujeto activo.

Ahora bien, y situándonos en el caso concreto del tipo penal del art. 173, inc. 16, del Código Penal -la comúnmente llamada "estafa informática"- es fácil advertir, primariamente, una diferencia sustancial con respecto a la modalidad defraudatoria mediante el empleo de *phishing* que venimos analizando. Para dar curso a este análisis, vamos a comenzar por la modalidad comisiva que caracteriza a la estafa informática.

B. Verbos típicos ¿Hay manipulación informática o es manipulación, a través de medios informáticos?

La acción genérica que describe el art. 173, inc. 16, del Código Penal es defraudar mediante la manipulación de un ordenador o los datos transmitidos[30].

En este caso, el tipo objetivo se dice que incrimina las defraudaciones cometidas mediante cualquier técnica de manipulación informática que implique una modificación del resultado con respecto a un proceso automatizado de datos. Es decir, que se produzca a través de la introducción de nuevos datos y/o de la alteración de los existentes, en cualquiera de las fases correspondientes a su tratamiento o procesamiento[31].

Con relación a este tipo penal, existen dos (2) grandes posturas a nivel doctrinario.

Por un lado, como ya fue señalado, un sector de la doctrina dentro de la Cámara de Apelaciones de la Justicia Nacional en lo Criminal y Correccional ha señalado lo siguiente: "…los sucesos investigados no se encuentran controvertidos pues los impugnantes circunscriben sus agravios al sostener la ausencia del aspecto subjetivo que reclama el tipo previsto por el art. 173, inciso 16, del Código Penal. Cabe recordar que la pesquisa versa sobre las 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

[30] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 171.
[31] ZAFFARONI, Raúl Eugenio y; BAIGÚN, David. "Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial. Tomo VII". Editorial Hammurabi. Pág. 277.

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 (…) La cercanía temporal entre las operaciones referidas y su extracción (...) en tanto concurrieron en la misma fecha de la transacción a retirar valores, permiten inferir que actuaron en pleno conocimiento y voluntad de llevarla a cabo…"[32]. En tal sentido, afirmaciones como la precedente se han vinculado a sucesos calificados como defraudaciones mediante manipulación de un sistema informático[33].

Contrariamente, la postura mayoritaria en el seno de la doctrina nacional -con el que acordamos a los fines del presente trabajo- se pronuncia en contra de dicha opinión, afirmando que este tipo penal sólo contiene a las defraudaciones "…que alteran el normal funcionamiento del sistema informático, la transmisión de datos, no aquellas en que la defraudación, que es en definitiva aquí la transferencia o disposición patrimonial, es ejecutada por la propia víctima engañada por el autor a través de medios informáticos, en cuyo caso podrá tratarse de una estafa del art. 172"[34].

En igual sentido, el Dr. Palazzi, afirma que "…la reforma apuntó no sólo a procesos informáticos que son modificados, sino a cualquier supuesto de defraudación mediante ordenadores, como accesos ilegítimos mediante claves falsas o phishing o falsos montajes en cajeros automáticos que quedan cubiertos por esta figura y, con anterioridad a la reforma, estaban incluidos en la figura general del art. 172, Cód Penal, o del art. 173, inc. 15, Cód. Penal.

Se trató de una opción muy importante del legislador, porque dentro de la estafa informática para el derecho comparado también quedan incluidas las figuras relacionadas con cualquier alteración o uso de la informática, como el caso del phishing, así decidido por la jurisprudencia comparada. Es una suerte de tipo penal abierto en relación con cualquier abuso informático (…) No quedan incluidos dentro de este supuesto los casos de ingeniería social, donde el autor con cierta habilidad se hace dar la clave de acceso a un sistema informático, ya sea telefónicamente o mediante phishing"[35]. Concretamente,

[32] Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala IV. Causa nro. 34.255/2018, caratulada "Betancourt Yésica y otros s/ procesamiento del 13/11/2018.
[33] Íbidem.
[34] RODRÍGUEZ, Pedro. "Casos especiales de defraudación. Código Penal Comentado de Acceso Libre" en Revista de Derecho Penal, Asociación Pensamiento Penal. Pág. 31.
[35] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 171.

en el *phishing defraudatorio*, no se altera el normal funcionamiento de un sistema informático: razón por la cual, no queda comprendido dentro de los supuestos de estafa informática[36].

Vale la pena destacar cuál es la circunstancia que asemeja al tipo penal de la defraudación informática -art. 173, inc. 16°, del Código Penal- con la estafa común del art. 172 del Código Penal.

En este sentido, tanto la estafa, como la defraudación por medio de computadoras, tienen que fundamentar la responsabilidad del autor por una transmisión patrimonial que puede imputarse formalmente como disposición al titular del patrimonio, pero que es contraria a su verdadera voluntad[37]. Es decir, es la víctima -o el sistema informático que es de su propiedad- la que efectúa el acto de disposición, pero tal acto se encuentra viciado con motivo del *error* bajo el cual opera el sujeto pasivo. Es así como, en la estafa, la disposición misma permanece en manos del damnificado, pero ésta se realiza toda vez que actúa engañado[38].

Por otra parte, en el caso concreto de la defraudación por medio de computadoras, junto a la falsificación de la base de información mediante la presentación de datos incorrectos o incompletos, se prevé también la posibilidad de falsificar "las máximas de la disposición". Esto significa que el autor puede llevar a cabo dicha disposición mediante la manipulación del programa utilizado por la víctima: que ya no se desapodera a sí misma, sino que resulta lesionada en su patrimonio a través de la manipulación de un sistema informático que actúa "engañado". En estos casos, el autor también podrá modificar las condiciones de una disposición prevista por el titular mediante la vía de un influjo "físico" sobre el desarrollo del procesamiento de datos. De esta forma, el tipo penal del art. 173, inc. 16, comprende maniobras realizadas sobre la manipulación del propio *hardware* empleado por la víctima[39].

De lo anterior, se desprende que el empleo de "…cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos" sea considerado, por parte de la doctrina, como un requisito de

[36] Íbidem.
[37] KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002. Pág. 167.
[38] Íbidem.
[39] Íbidem.

tipicidad objetiva[40] cuando hablamos de defraudación informática. Ya que, de verificarse la ausencia de tales circunstancias, no podríamos afirmar que nos encontráramos ante un supuesto en el que se verifica la presencia del tipo penal bajo análisis.

Ahora bien, y amén de todo lo analizado con relación al *phishing defraudatorio*, estamos en condiciones de afirmar que esto último no siempre se cumple. En tal sentido, es sencillo imaginarnos que, en el ejemplo hipotético de quién -a través de medios informáticos-, engaña a la víctima haciéndose pasar por una autoridad bancaria[41]: no se cumple el requisito de tipicidad objetiva ya señalado debido a que el autor no utiliza *malware*[42], modificaciones de *hardware*, ni ninguna otra herramienta destinada a tal efecto. Concretamente, el autor de tal delito no realiza ninguna maniobra "…que altere el normal funcionamiento de un sistema informático o la transmisión de datos" tal como requiere el tipo penal del art. 173, inc. 16.

Con relación a la modalidad comisiva que define a este tipo penal, usualmente se emplea el término "*ardid informático*". Lo anterior, toda vez que los ordenadores y sistemas informáticos toman decisiones constantemente, lo que posibilita la realización de un ardid tendiente a desviar el curso normal de dichas decisiones ("normal" en tanto son aquellas decisiones que lícitamente le ordena al sistema un usuario autorizado). En dicha medida, se ha dicho que actúan casi como la mente humana, pero de forma mucho más limitada, ya que están programados para actuar frente a acciones o pedidos y ejecutar un determinado comando[43].

La manipulación a la que hace referencia el tipo penal descripto debe alterar el funcionamiento del sistema informático. Concretamente, no es cualquier manipulación informática, sino sólo la que es apta para producir dicho efecto. Si por un error en la programación ello no sucede, estaremos ante un delito tentado o uno imposible[44].

[40] TAZZA, Alejandro. "Código Penal de la Nación Argentina. Comentado. Tomo II". Rubinzal-Culzoni Editores. Santa Fe 2018. Págs. 202-203.
[41] Nótese que este ejemplo, en su estructura, coincide con aquel analizado por la Cámara Nacional de Apelaciones en lo Criminal y Correccional, en el marco de la Causa Nro. 60.479/2019/TO1, caratulada "Narciso Yedros, Fabián s/ estafa -procesamiento-".
[42] Un software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.
[43] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 172.
[44] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 172.

Es así que, claramente, el mencionado *ardid informático* poco tiene que ver con el *engaño* o *ardid* requerido por la estafa del art. 172 del Código Penal.

A modo de ejemplo, un caso común de defraudación informática sería el siguiente: una persona ingresa a un comercio de gastronomía y, previo a realizar su pedido, se conecta a la red wifi del establecimiento. Al conectarse a dicha red, un tercero logra *hackear* su sistema informático y realizar modificaciones en la plataforma de homebanking de la víctima para que, cada vez que ésta efectúa una transferencia, se realice un desvío de fondos a la cuenta del autor del hecho. Sin notar nada extraño, efectúa una consumición en el lugar y, a la hora de pagar, decide hacerlo a través de su cuenta bancaria. Sin saber que, con motivo del *hacking*, cada transferencia realizada se duplica hacia la cuenta del autor. Horas más tarde, se percata de que se han realizado una serie de desvíos de fondos desde su cuenta bancaria en favor del autor del delito en cuestión. El ejemplo citado está basado en los hechos ocurridos en un caso real[45]. Sucesos de tales características, han sido catalogados como defraudaciones informáticas conforme art. 173, inc. 16, del Código Penal.

Nótese a través del ejemplo señalado, tal y como lo previó el legislador al momento de sancionarse la Ley 26.388, la semejanza que existe entre la defraudación informática y la defraudación mediante el uso no autorizado de tarjeta de débito o crédito del art. 173, inc. 15, del Código Penal[46]. Si bien ambos tipos penales son semejantes en cuanto a su estructura típica: ninguno de ellos requiere que el acto de disposición patrimonial sea llevado a cabo por la víctima en los términos requeridos por la estafa común. Presentan una diferencia sustancial en cuánto al medio utilizado por el autor para llevar a cabo la conducta defraudatoria.

En el caso del art. 173, inc. 16, se utilizan herramientas -tanto de *hardware* como de *software*- que permitan engañar a un sistema informático y/o la transmisión de datos: al menos en la parte que refiere a la disposición patrimonial. Mientras que en el caso del art. 173, inc. 15, se requiere de la capacidad del autor de acceder a las credenciales bancarias contenidas en una tarjeta de débito o crédito a través de cualquiera de los medios

[45] Cámara Nacional de Apelaciones en lo Criminal y Correccional. Causa nro. CCC 33.241/2022 caratulada "G.A.J. s/ defraudación informática, en calidad de autora".
[46] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Págs. 157-159

contenidos en el tipo: falsificación, adulteración, robo, hurto, apropiación, o a través del uso no magnetizado de sus datos.

En síntesis, estamos en condiciones de afirmar que, en este punto, es posible realizar la siguiente distinción: **i)** por un lado se encuentran las defraudaciones informáticas -como las que están comprendidas por el tipo penal del art. 173, inc. 16, del Código Penal-, y **ii)** por otra parte, tenemos a las defraudaciones que se ejecutan a través de medios informáticos, ya que el autor utiliza tales herramientas para, por ejemplo, entablar contacto con la víctima, pero no para modificar "las máximas de la disposición" como ya referimos.

De este modo, podemos sencillamente concluir que el tipo penal señalado no comprende a la modalidad delictiva del *phishing defraudatorio* en los términos que venimos analizando. Lo anterior, toda vez que, la estafa informática se centra en defraudaciones que implican la alteración del normal funcionamiento de un sistema informático y/o la transmisión de datos que, a su vez, ocasionan un perjuicio patrimonial para la víctima.

Amén de lo expuesto, se torna necesario citar la postura doctrinaria del Dr. Palazzi cuya opinión fuera señalada al inicio de este acápite que refiere, con relación al tipo penal del art. 173, inc. 16, que "No quedan incluidos dentro de este supuesto los casos de ingeniería social[47], donde el autor con cierta habilidad se hace dar la clave de acceso a un sistema informático, ya sea telefónicamente o mediante phishing"[48]. Siendo que son, precisamente, aquellos casos de ingeniería social los que caracterizan a la modalidad delictiva del *phishing defraudatorio*.

[47] Esto es, obtener información confidencial a través de la manipulación de usuarios legítimos. El principio que sustenta la ingeniaría social es que, en cualquier sistema, 'los usuarios son el eslabón débil'.
[48] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Págs. 173-174.

IV. Análisis del Art. 172 y su relación con el *phishing*.

A. Elementos constitutivos y evolución legislativa.

Antes de avanzar sobre las últimas modificaciones legislativas que este tipo penal ha recibido, no sólo a nivel nacional, sino también en países como Alemania y España, vale la pena hacer una breve reseña histórica acerca de las primeras nociones de esta conducta.

En este sentido, el profesor Edgardo Donna nos recuerda que el fraude fue castigado no sólo por el Derecho Romano, de donde, en principio, proviene como figura de los Derechos modernos, sino que también se encontraba legislado en otros países. La ley babilónica de Hammurabi (s. XX a. C), el Avesta Persa, el libro del profeta Amos, el Corán, el Códigos de Manú, tenían penas severas; en algunas de estas legislaciones, la de muerte[49].

En el Código Penal Argentino, el tipo penal de la estafa se encuentra incluido en el Título VI, denominado "Delitos contra la Propiedad". Sin embargo, basta con analizar el contenido de los diferentes tipos para reconocer que en realidad la protección legal va mucho más allá que el mero "derecho de propiedad"[50].

Tal es así que un sector mayoritario de la doctrina afirma que resulta más adecuado hablar de "delitos contra el patrimonio", pues no sólo se incluyen acciones que lesionan o ponen en peligro a la propiedad, sino también aquellas que afectan a otros valores patrimoniales como la posesión, el derecho de crédito, e incluso las expectativas[51].

A diferencia de otros tipos penales, como el hurto o el robo, en el caso de la estafa la distinción es aún más evidente, pues no se protege un determinado elemento integrante

[49] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 256-257.
[50] TAZZA, Alejandro. "Código Penal de la Nación Argentina Comentado. Parte Especial. Tomo II". Segunda edición, actualizada. Rubinzal-Culzoni Editores. Santa Fe, 2018. Págs. 7-8.
[51] TAZZA, Alejandro. "Código Penal de la Nación Argentina Comentado. Parte Especial. Tomo II". Segunda edición, actualizada. Rubinzal-Culzoni Editores. Santa Fe, 2018. Págs. 7-9.

del patrimonio, sino que se toma en cuenta al patrimonio de la víctima como una unidad o conjunto[52].

En el ámbito comparado, la doctrina española ha llegado al extremo de afirmar que los delitos contra el patrimonio son aquellos que atentan al mismo considerado como valor económico y que es perjudicado por la acción delictiva, estimándose como prototipo de ellos la estafa, que es el delito patrimonial por antonomasia, hasta el punto de llegar a afirmarse, no sin exageración, que el concepto de patrimonio -en los términos requeridos por el Derecho Penal- nace por y para este tipo penal y se desarrolla a partir de sus exigencia[53].

Concretamente, y de forma unánime, la doctrina nacional sostiene que los cuatro (4) elementos que constituyen a la estafa del art. 172 del Código Penal, son los siguientes: **i)** la existencia de un ardid o engaño que conduce a la víctima al **ii)** error que la lleva a realizar uno o más actos de **iii)** disposición patrimonial, mediante lo cual se le ocasiona un **iv)** perjuicio patrimonial[54]. Dichos elementos deben darse en ese orden y vincularse por una relación de causalidad, o si se prefiere, de imputación objetiva.

A continuación, veremos que el *phishing defraudatorio* comparte la mayoría de estos elementos, no así el tercero, y vamos a estudiar qué problemática encierra aquello.

B. Ardid o engaño a través de medios informáticos.

Como ya fue señalado, el ardid o engaño son las dos (2) únicas modalidades comisivas previstas en la ley para caracterizar a la estafa, de ahí que siempre se tornó fundamental precisar correctamente tales conceptos a fin de garantizar plenamente el principio de legalidad[55]. En lo referente a este trabajo, este acto de definir y precisar tendrá un objetivo adicional que es, como ya se dijo, reforzar las nociones existentes en torno a los múltiples puntos de contacto entre la modalidad comisiva del *phishing* y el tipo penal de estafa del art. 172 del Código Penal.

---

[52] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 263.
[53] CONDE-PUMPIDO FERREIRO, Cándido. "Estafas". Tirant Lo Blanch. Valencia 1997. Pág. 33.
[54] TAZZA, Alejandro. "Código Penal de la Nación Argentina Comentado". Rubinzal-Culzoni Editores. Buenos Aires 2018. Págs. 111-113.
[55] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 273.

En concreto, si afirmamos que existe una relación de especificidad entre el *phishing*, por un lado, y el *ardid* o *engaño*, por otro: no nos quedaría más opción que afirmar que el *phishing defraudatorio*, sí encuentra arraigo en el tipo penal del art. 172 del Código Penal. Lo anterior, debido a que compartirían una misma modalidad comisiva, ya que, a fin de cuentas: ambas son defraudaciones. A continuación, veremos qué sucede.

Volviendo a lo expresado en el primer párrafo, nos ilustra Antón Oneca al afirmar que el engaño es la simulación o disimulación capaz de inducir a error a una o varias personas[56].

En esta línea de pensamiento, existen dos (2) criterios en pugna con relación a cómo se debe entender el engaño.

En primer lugar, existe el denominado *criterio limitado*, según el cual el engaño como elemento típico fundamental va a exigir una especial maquinación o puesta en escena. Concretamente, el medio engañoso debe adoptar cierta entidad, no resultando suficiente con las simples palabras, sino que en todos los casos el autor debe desplegar alguna actividad tendiente a falsear la verdad[57].

Esta tesis atiende "…al revestimiento exterior del engaño: se incrimina el engaño que esté construido con una cierta riqueza de formas y de medios; se exige que el motivo fraudulento no venga simplemente enunciado, sino que venga desenvuelto y revestido de un acompañamiento de maquinaciones aptas para abrir una brecha en la defensa del sujeto pasivo"[58].

La principal crítica que recibe dicha teoría refiere a que no contempla que, en la estafa, lo que se castiga no es el engaño en sí, sino la lesión patrimonial que dicho engaño ocasiona. Por lo que no resulta de particular importancia el modo en que se logró el daño patrimonial, es decir, si el error inducido en la víctima es producto de un medio refinado o simple. El artificio es irrelevante mientras el bien jurídico lesionado sea la propiedad[59].

---

[56] ANTON ONECA, José. "*Las estafas y otros engaños, en el Código penal y en la jurisprudencia*". Anuario de Derecho Penal y Ciencias Penales (1958). Pág. 80.
[57] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 275-276.
[58] PEDRAZZI, Cesare. "Inganno ed errore nei delitti contro il patrimonio". Dot. A. Giuffré Editore. Milano 1955. Pág. 220.
[59] RODRÍGUEZ, Pedro. "Estafas y otras defraudaciones. Código Penal Comentado de Acceso Libre" en Revista de Derecho Penal, Asociación Pensamiento Penal. Págs. 9-10.

En segundo lugar, tenemos al denominado *criterio amplio*, que considera que para la existencia del delito de estafa es suficiente con cualquier forma de engaño que sea idónea para inducir a error a la víctima, sin que en todos los casos sea exigible el despliegue de alguna maniobra o actividad fraudulenta exterior. Es decir, para estimar el carácter penal del delito basta con que la conducta, aunque sólo se encierre en una mentira verbal, sea susceptible de engañar a la persona a la que va dirigida, o que el engaño no sea fácilmente verificable[60].

Esta última parece haber sido la tesis adoptada por nuestro Código Penal, ya que el art. 172 utiliza como posibles formas de comisión del delito, no sólo al engaño, sino también al ardid -forma más compleja del primero-[61]. Este último es entendido como el empleo o utilización de medios artificiosos para deformar la realidad, ya sea simulando aquello que no existe u ocultando lo que sí[62].

Independientemente del criterio adoptado, es evidente que cualquiera de ellos sirve para explicar lo que bien podría ser alguna de las modalidades comisivas más comunes observadas en casos de *phishing*. Sin ir más lejos, varias de ellas se encuentran directamente detalladas en nuestro derecho sustantivo, como repasaremos a continuación.

Nuestro Código Penal adopta como técnica legislativa la de enunciar ejemplos concretos de ardid o engaño, a saber: *nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, créditos, comisión, empresa o negociación*. Con relación a esto, repasaremos brevemente cada uno de estos ejemplos.

Se afirma que existe nombre supuesto cuando el autor, para simular que es otra persona, se presenta ante la víctima con un nombre que no es el real o el que habitualmente usa, generando, consecuentemente, un error sobre su identidad. En el marco de una conducta de *phishing*, podría ocurrir en el supuesto de quien refiere ser el gerente de una determinada entidad bancaria y, para corroborar sus dichos, invita a la víctima a ingresar al sitio web de la entidad bancaria que se trate a los fines de corroborar dicha información (lo anterior, toda vez que las entidades bancarias tienen la obligación de publicar el nombre y apellido de los gerentes de sus distintas sucursales en el sitio web oficial).

[60] CONDE-PUMPIDO FERREIRO, Cándido. "Estafas". Tirant Lo Blanch. Valencia 1997. Pág. 49.
[61] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 279.
[62] Íbidem.

Por calidad se entiende aquí el estado, la situación personal, la condición que tiene un individuo en las relaciones de familia, o sus condiciones jurídicas o sociales en general (estado de esposo o pariente, cargos, dignidades, funciones, nacionalidad, etcétera). Trátase de una atribución actualmente falsa, que puede obedecer a una simulación total (invocar un cargo que no se tiene) o a la invocación de una calidad que se ha tenido, pero que ya no se tiene, o que se va a tener pero que todavía no se posee. Como en el caso anterior, la simulación debe inducir a la víctima a un error que lo impulse a hacer la disposición patrimonial; no queda comprendida la que sólo se emplea para facilitar el contacto personal o la permanencia en determinado lugar (p.ej., en una sala de remate de acceso restringido), es decir, cuando la invocación de la calidad no haya sido determinante de la prestación no compensatoria[63]. Un caso como éste sería aquel mediante el cual, el *phisher*, intenta valerse de una determinada (y falsa) urgencia -como ser una próxima e inminente devaluación, respecto de la cual tiene conocimiento por algún contacto- para hacerle creer a la víctima que ambos tienen un lazo familiar -existen casos de *phishers* que logran hacerle creer a la víctima que se trata de su hijo, o sobrino, también se emplean técnicas para modificar las voces humanas en casos de llamados telefónicos- que, en rigor de verdad, es falso.

El empleo de falsos títulos es, en resumidas cuentas, la simulación de una calidad representada por un título otorgado o reconocido por el Estado (p.ej., títulos profesionales), instituciones universitarias (grados meramente académicos), culturales (distinciones honoríficas) o reconocidos por la costumbre (títulos de nobleza), etc., nacionales o extranjeros, correspondientes a la realidad o totalmente inexistentes (p.ej., invocar el doctorado de una universidad que no existe), cuya utilización determina la prestación no compensatoria. Cuando la realización del ardid constituido por el empleo del falso título implique, a la vez, el uso público que reprime el art. 247 del Cód. Penal, puede darse un concurso ideal entre ambas figuras[64]. En una maniobra de *phishing*, este ejemplo sería similar al primero, refiere al *phisher* que se arroga títulos y condiciones que no posee -como ser gerente de una entidad bancaria, empleado de una plataforma de pagos, bróker financiero, etc.-.

[63] CREUS, Carlos. "Derecho Penal. Parte Especial. Tomo I – 6ta edición actualizada y ampliada". Editorial Astrea. Buenos Aires, 1997. Pág. 470.
[64] CREUS, Carlos. "Derecho Penal. Parte Especial. Tomo I – 6ta edición actualizada y ampliada". Editorial Astrea. Buenos Aires, 1997. Pág. 471.

La influencia significa aquí todo poder o valimiento que se tenga entre personas, grupos o componentes de una institución, y es mentida cuando el agente no la posee efectivamente. Cuando el agente la posee y la invoca para que el sujeto pasivo realice la prestación no compensatoria, sin intención de hacerla valer como lo dice, podrá tratarse de un engaño, pero no de un caso de influencia mentida[65].

No se trata aquí del abuso de la confianza originada en un negocio jurídico. Ésta no es una figura de abuso de confianza, según la clasificación precedentemente realizada, sino de fraude. Aquí el abuso de confianza constituye un ardid y, como tal, exige un despliegue de actividad destinada a engañar. Y puesto que se trata de un abuso, tanto puede referirse a una confianza suscitada por el mismo agente que persigue el logro de la prestación no compensatoria (p.ej., promesa de matrimonio para obtener dinero con miras a supuestas inversiones comunes futuras), como de una confianza ya existente que el agente aprovecha engañosamente en un determinado momento (invocar la amistad para que el amigo pague una deuda inexistente y quedarse él con el dinero).

Aparenta el que muestra algo que no se condice con la realidad; se trata, pues, de simular[66]. La generalidad de la doctrina requiere la exhibición (exterior) falsa, o sea, que se trate de una apariencia ardidosa; sin embargo, no pocos admiten la forma puramente engañosa (p.ej., una manifestación de bienes mentirosa, en determinadas circunstancias, puede constituir perfectamente la apariencia fraudulenta).

En primer término, se dice que aparenta bienes el que muestra que tiene cosas o derechos que en realidad no integran su patrimonio[67]. Aparenta crédito el que simula la obtención de un respaldo económico de terceros. Aparenta empresa, quien simula la existencia de una organización destinada a la producción económica lucrativa, la reunión de medios económicos sin fines de lucro (p.ej., una fundación de bien público) o muestra como existentes características que una empresa real no tiene.

En igual sentido, aparenta negociación el que simula la existencia de una transacción que se realiza o se va a realizar, o muestra características distintas de una transacción que se está llevando o se llevó a cabo.

[65] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 297-298.
[66] TAZZA, Alejandro. "Código Penal de la Nación Argentina Comentado. Parte Especial. Tomo II". Segunda edición, actualizada. Rubinzal-Culzoni Editores. Santa Fe, 2018. Págs. 126-128.
[67] Ibidem.

Por último, se dice que aparenta comisión el que simula cualquier especie de representación de un tercero para realizar un acto o llevar a cabo un hecho o exhibe una extensión de esa representación distinta de la que realmente se le ha otorgado[68].

Amén de todo lo expuesto, es sencillo entender que todas las modalidades comisivas reseñadas hasta aquí (y narradas por el propio texto legal que compone al art. 172 del Código Penal), son habitualmente utilizadas en las maniobras de *phishing*. Ahora bien, lo que distingue a esta modalidad delictiva de los ejemplos comúnmente brindados por la doctrina experta en la materia, radica en el medio y en el objeto de esta modalidad delictiva ¿Qué se quiere decir con esto?

Rara vez el autor de una maniobra de *phishing* se encuentra cara a cara (existen algunos pocos casos en los cuáles tal encuentro puede tener lugar a través de una aplicación como Zoom, Google Meets, etc.) con la víctima. El contacto entre sujeto activo y pasivo se suele dar a través de medios informáticos como pueden ser redes sociales, mensajes a través de correo electrónico, aplicaciones de mensajería instantánea, etc.

Sin perjuicio de lo anterior, resulta evidente que, si tomamos el *criterio amplio* reseñado previamente, sí se puede afirmar que el *phishing*[69] no presenta grandes diferencias con relación a la modalidad comisiva de ardid o engaño requerida para la estafa común. Concretamente, en caso de que el *phisher* se comunique con la víctima, haciéndose pasar por un tercero, con el fin de obtener información confidencial perteneciente a la misma: estaría realizando un ardid o engaño mediante el empleo de nombre supuesto y/o calidad simulada, como requiere este tipo penal.

Ahora bien, la principal dificultad no radica en el error al cual la víctima es inducida con motivo del ardid o engaño, sino el siguiente elemento constitutivo de este tipo penal. Elemento que analizaremos en el siguiente acápite de este trabajo.

[68] CREUS, Carlos. "Derecho Penal. Parte Especial. Tomo I – 6ta edición actualizada y ampliada". Editorial Astrea. Buenos Aires, 1997. Pág. 472.

[69] En tanto "…*maniobra tendiente a la obtención de información confidencial de terceros, mediante técnicas de ingeniería social que involucran correos electrónicos, sitios web o perfiles en redes sociales engañosos, en los que los autores se hacen pasar por terceros*" como definimos al inicio.

C. Vínculo existente entre la estafa y el *phishing*: el acto de disposición.

Como ya fue señalado, la principal problemática que introduce el *phishing defraudatorio* cuando se lo vincula con el tipo penal de la estafa del art. 172 del Código Penal radica en su tercer elemento constitutivo: la necesidad de que exista un acto de disposición patrimonial realizado por parte de la víctima.

El tipo penal de la estafa exige que, como consecuencia del error, la víctima del engaño realice un acto de disposición patrimonial. Éste, a su vez, debe ser causa del perjuicio patrimonial[70].

En dicho sentido, la doctrina sostiene que nos encontramos en presencia de un requisito que le atribuye una connotación especial a la estafa pues, a diferencia de otros delitos contra el patrimonio, para la configuración del tipo es ineludible una contribución especial de la víctima[71].

De tal modo, es imprescindible que la disposición patrimonial sea realizada por la misma persona que sufrió el engaño, pero en cambio, el acto de disposición puede generar un perjuicio patrimonial propio o ajeno, de modo que no necesariamente debe coincidir la identidad de quien dispone movido por error, y quien en definitiva resulta perjudicado[72].

Ahora bien, ya hemos afirmado que el *phishing* es una "maniobra tendiente a la obtención de información confidencial de terceros, mediante técnicas de ingeniería social que involucran correos electrónicos, sitios web o perfiles en redes sociales engañosos, en los que los autores se hacen pasar por terceros".

Empero, al vincular al *phishing* con la estafa común del art. 172 del Código Penal, parte de la doctrina ha planteado -como ya hemos visto- que éste se asemeja en gran medida a las modalidades comisivas de ardid o engaño que definen a este tipo penal. Ahora bien, al momento de realizar una comparación con relación al *phishing defraudatorio* que definimos al inicio de este trabajo, se observan algunas diferencias. Para entenderlo más sencillamente, ilustraremos lo señalado a través de un ejemplo.

[70] RODRÍGUEZ, Pedro. "Estafas y otras defraudaciones. Código Penal Comentado de Acceso Libre" en Revista de Derecho Penal, Asociación Pensamiento Penal. Págs. 8-9.
[71] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 315.
[72] CONDE-PUMPIDO FERREIRO, Cándido. "Estafas". Tirant Lo Blanch. Valencia 1997. Pág. 49.

Volviendo al caso más común, si el sujeto activo aborda a la víctima haciéndose pasar por un funcionario o autoridad de una institución bancaria a fin de que el sujeto pasivo le brinde sus claves personales: lo que habría aquí no sería un acto de disposición patrimonial *per se*. Se afirma lo anterior ya que, es imposible afirmar que nuestras claves o datos personales tengan, necesariamente, entidad patrimonial. En síntesis, lo que sucede en la mayoría de los casos de *phishing defraudatorio* -que, por cierto, se asemeja a la estafa en todos sus elementos- es lo siguiente: **i)** el sujeto activo dirige un ardid o engaño hacia la víctima con el objeto de que ésta incurra en un **ii)** error que la lleve a realizar un **iii)** acto de disposición -no patrimonial-, que le ocasiona un **iv)** perjuicio patrimonial.

Es decir, y para responder a la pregunta formulada en el acápite precedente relativa a si existe una relación de especificidad entre el *phishing*, por un lado, y el *ardid* o *engaño*, por otro: la respuesta parecería ser no. Y la fundamentación radicaría, precisamente, en que el *phishing* posee este elemento adicional que le brinda al sujeto activo una posición ventajosa respecto al patrimonio del damnificado; circunstancia que no ocurre en los demás casos de ardid o engaño.

Aquí, nuevamente, vamos a encontrarnos con otra dificultad a raíz de las diversas opiniones doctrinarias al respecto.

Por un lado, el Prof. Edgardo Donna, afirma lo siguiente con relación a la disposición patrimonial, afirmando que: "Este elemento de la estafa debe ser entendido en sentido amplio. No consiste únicamente en la entrega de una cosa, sino que debe incluirse en el concepto de disposición patrimonial cualquier otra decisión con consecuencias patrimoniales perjudiciales, ya sea que recaiga sobre bienes muebles, inmuebles, derechos de contenido patrimonial o en la prestación de servicios, siempre que tengan un valor económico"[73]. De esta forma, existe un sector de la doctrina que sostiene un *criterio amplio* con relación a dicho elemento.

Ahora bien, existen otros juristas que no comparten esta postura, en concreto, Creus afirma que el "…patrimonio se ve disminuido, después de ese momento, por la disposición patrimonial realizada por el sujeto pasivo del engaño, es decir, por su acción u omisión, que puede ser un acto jurídico (firmar un contrato), o un simple hecho (dar

[73] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 315.

algo), que puede crear derechos de terceros sobre el patrimonio o extinguir deudas de terceros en favor del patrimonio"[74].

Esta postura se deriva de la expresada por Soler: "La estafa es un delito para cuyo perfeccionamiento se requiere la efectiva producción de un daño. Ese daño debe estar constituido o derivar directamente de la disposición patrimonial erróneamente tomada por el engañado, sea con respecto al propio patrimonio, sea en relación al de un tercero del cual puede disponer"[75].

Amén de lo expuesto, vale la pena remarcar que sólo a través la interpretación de Donna se podría justificar que la modalidad delictiva del *phishing* mantiene una relación de especificidad con el ardid y/o engaño. Y, por consiguiente, que el *phishing defraudatorio* pueda encontrar arraigo en la calificación legal de la estafa conforme art. 172 del Código Penal.

En su hipótesis, Donna toma la postura esbozada por Bajo Fernández y Pérez Manzano, que refieren que: "El acto de disposición puede consistir tanto en hacer entrega o de gravar una cosa, como en prestar un servicio, como en realizar la prestación a la que se ha obligado en el contrato. Comete estafa quien logra, mediante engaño bastante e idóneo, obtener un servicio de un médico con ánimo de no pagar. El servicio del médico es un acto de disposición patrimonial porque implica la realización de un comportamiento con valor económico (Manual de Derecho Penal cit., p. 284, y en similares términos GONZÁLEZ RUS, Derecho Penal, p. 668). Entre nosotros ya había afirmado Núñez que "existe una disposición de propiedad con arreglo al art. 172, si el ofendido por la estafa u otra persona hace u omite algo que priva de su propiedad al primero, en beneficio del autor del delito o de un tercero. Ese algo puede ser un simple hecho, por ejemplo realizar sin la debida compensación un trabajo pecuniariamente valioso, o puede ser un acto jurídico de transferencia de la propiedad o de renuncia a ella [...] Así, la estafa puede recaer sobre bienes tales como la tenencia o posesión de una cosa mueble o su dominio; las ventajas económicas correspondientes a una explotación comercial o la indemnización pertinente a su frustración; el beneficio jubilatorio; el valor de servicios o alimentos; la garantía susceptible de valor pecuniario que significa un embargo, la inhibición o el

[74] CREUS, Carlos. "Derecho Penal. Parte Especial. Tomo I – 6ta edición actualizada y ampliada". Editorial Astrea. Buenos Aires, 1997. Pág. 465.
[75] SOLER, Sebastián. "Derecho Penal Argentino. Tomo IV". Tipográfica Editora Argentina. Buenos Aires 1992. Pág. 370.

documento de prenda agraria, o el valor de un crédito" (ob. cit, p. 287). En igual sentido, según Soler, "la disposición tomada puede consistir en la entrega de una suma de dinero, de una cosa, mueble o inmueble, de un derecho y también del despliegue de un trabajo que se entiende retribuido, o de un servicio tarifado [...] también en la renuncia a un derecho" (ob. cit., p. 370), y en forma coincidente se expiden Molinario-Aguirre Obarrio al incluir en la tutela a cualquier aspecto integrante del patrimonio de las personas"[76].

De este modo, se deduce que existen posturas doctrinarias que permiten interpretar al *phishing*, ya no sólo como una antesala, sino como una modalidad comisiva con relación a la estafa común del art. 172 del Código Penal. Ahora bien, esto parecería no resultar suficiente para superar la discusión en torno a la practicidad y conveniencia de contar con una norma más específica que contenga a dicha modalidad delictiva.

D. ¿Puede la modalidad delictiva del *phishing* ser interpretada como una estafa en grado de tentativa?

Si compartimos el *criterio amplio*[77] establecido por el Prof. Edgardo Donna con relación al tercer elemento constitutivo de la estafa común, es decir, la necesidad de que exista un *acto de disposición patrimonial* por parte de la víctima; es posible afirmar, entonces, que el phishing defraudatorio puede ser calificado como estafa común. Ahora bien, resta analizar, en tal caso, cómo se interpretaría el *phishing* en el marco de una tentativa de dicho delito.

Con relación a la tentativa de la estafa común y tomando como basamento, nuevamente, la postura del Dr. Donna, se ha dicho: "La tentativa se inicia con la ejecución de la conducta engañosa, pero es imprescindible que el ardid o engaño cumplan con todos los requisitos de idoneidad analizados. Por ello, si la acción no llega a vulnerar los 'usos y costumbres sociales vigentes en el tráfico', no es posible afirmar siquiera la tentativa, pues no puede decirse que haya habido un comienzo de la ejecución del delito (…) Obviamente la sola preparación de los instrumentos del engaño (por ej., falsificación del

[76] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 315-316.
[77] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 315.

documento) constituyen meros actos preparatorios impunes como estafa, salvo la falsificación, sin perjuicio de su adecuación a otro tipo penal"[78].

En el acápite anterior, hemos afirmado que -tomando el *criterio amplio* a los fines de evaluar el ardid o engaño, y tomando nuevamente el *criterio amplio* con relación al acto de disposición patrimonial- se puede interpretar que el *phishing defraudatorio* que hemos definido al inicio del presente trabajo: encuentra arraigo en el tipo penal del art. 172 del Código Penal, esto es, la estafa común.

Tomando el criterio esbozado en los párrafos precedentes, habiendo ya afirmado que el *phishing* opera como antesala para la comisión de otros delitos[79] y que, como modalidad comisiva, puede ser interpretado como ardid o engaño con relación a la estafa común -art. 172 CP-: podemos concluir que el *phishing* es suficiente para configurar una estafa en grado de tentativa si el plan del autor así lo permite (como también podría ser tentativa de daño informático, según el caso). Para ilustrar brevemente lo anterior, y a modo de ejemplo, podemos imaginar el caso de un *phisher* que se comunica telefónicamente con una persona y, haciéndose pasar por un empleado de autoridad bancaria, le solicita su usuario de homebanking y contraseña. La víctima, en la creencia de que el engaño del autor resulta ser una afirmación verdadera, le facilita tales datos. Inmediatamente, el phisher corta la comunicación y se dispone a ingresar a la red homebanking de la víctima a los fines de consumar el perjuicio patrimonial: pero no lo logra debido a que tal red se encuentra en mantenimiento. En el mismo momento, la víctima se percata de lo sucedido y se comunica telefónicamente con la entidad bancaria para dar de baja su usuario de homebanking. Cuando se restaura el sistema, el *phisher* no logra ingresar debido a que el usuario que le fue suministrado se encuentra suspendido. Dicha conducta podría ser calificada como estafa en grado de tentativa -arts. 42 y 172 del CP-.

Ahora bien, no todos los casos de *phishing* en los cuáles el autor posea la finalidad de efectuar un perjuicio patrimonial -compatible con la estafa común- podrán calificarse de tal manera.

[78] DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001. Pág. 341.
[79] Y, conforme dicha noción, hemos afirmado que puede tratarse de un acto preparatorio o de un comienzo de ejecución según el delito del cual se trate y el plan del autor.

Por el contrario, en caso de no contar con una lesión al bien jurídico patrimonial se deberá analizar la puesta en peligro y la inmediatez temporal entre: **i)** la *pesca* de datos mediante técnicas de ingeniería social[80] y, **ii)** la puesta en peligro con respecto al bien jurídico patrimonial en cuestión.

En tal sentido, en aquellos casos en los cuáles el *phisher* se limite únicamente a la pesca de datos, pero no los utilice -con la inmediatez requerida- para la concreción de una lesión patrimonial: estaremos obligados a afirmar que se trató de un acto preparatorio y dicha conducta devendrá en atípica.

Por tal motivo, algunos países han sorteado dicha problemática mediante la adopción de tipos penales que regulan al *phishing* de manera autónoma.

En Argentina, al igual que en gran parte de otros países de Europa y el resto de la región, opera la prohibición general de penar actos preparatorios[81]. Dicha regla, admite dos (2) excepciones: a) el primer consiste en extender lo prohibido excediendo el ámbito de la tentativa hasta abarcar una parte de la actividad preparatorio, es decir, en alterar el alcance que tiene la fórmula general del art. 42 en su función de dispositivo amplificador de la tipicidad y; b) la tipificación independiente de ciertos actos preparatorios[82]. Algunas legislaciones han adoptado este segundo criterio.

Para reforzar esta noción, se van a traer a colación los ejemplos de España, de la República Federal de Alemania y los Estados Unidos.

En la legislación norteamericana se ha dotado a la modalidad delictiva del *phishing* de figuras que, en nuestro sistema, podrían ser clasificadas como *de peligro*[83].

De esta forma, el Código del Estado de Virginia considera al *phishing* como un delito de clase 6 y en su § 18.2-152.5:1 establece lo siguiente: "El uso de una computadora para recolectar información identificatoria; castigos. 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

[80] Conforme la definición brindada al inicio de este trabajo.
[81] ZAFFARONI, Raúl Eugenio; SLOKAR, Alejandro y; ALAGIA, Alejandro. "Derecho Penal. Parte General". Editorial Ediar. Buenos Aires 2002. Pág. 811.
[82] Ibidem.
[83] HILGENDORF, Eric y VALERIUS, Brian. "Derecho Penal. Parte General". Editorial Ad-Hoc. Primera Edición. Traducción de la 2da edición alemana. Buenos Aires, marzo del 2017. Pág. 18.

engaño, cualquier información identificatoria, como se define en cláusulas (iii) a (xiii) del inciso C del articulo § 18.2-186.3. Cualquier persona que no cumpla con 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"[84].

Otro caso similar, transcurre en el ámbito del Estado de Minnesota. En su estatuto, la norma Sub. d. 5 reza lo siguiente "Crimen de uso electrónico de falsa pretensión para obtener identidad: (a) Una persona que, con la intención de obtener la identidad de otra, usa una declaración falsa contenida en un correo electrónico dirigido a otra persona o en un sitio web, comunicación electrónica, propaganda, o cualquier otra comunicación en Internet, es culpable de delito. (b) Cualquiera que cometa dicho delito será sentenciado a prisión por un máximo de cinco años o al pago de multa por un monto no mayor a $10,000, o ambos"[85].

Por otra parte, en la legislación española, la estafa está regulada en el art. 248 del código sustantivo de ese país, que reza lo siguiente: "Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno".

En el caso señalado, se puede observar con toda claridad, que se ha eliminado el carácter de la *patrimonialidad* al acto de disposición que debe ser efectuado por parte de la víctima del delito de estafa.

Esta técnica legislativa, diferente a la adoptada en nuestro país con relación al tipo delictivo del art. 172 del Código Penal Argentino, resuelve una cuestión fundamental de cara a la modalidad delictiva del *phishing*, que es, precisamente, eliminar el conflicto en torno a qué características debe reunir el acto de disposición efectuado por la víctima que se desapodera a sí misma: lo anterior, sin la necesidad de recurrir a diversas posturas doctrinarias que habiliten su aplicación.

---

[84] https://virginiarules.org/varules_topics/technology-and-you/#:~:text=Phishing%20is%20prohibited%20by%20Code,deception%20to%20gather%20identifying%20information.

[85] https://www.revisor.mn.gov/statutes/cite/609.527#stat.609.527.5a

Por otra parte, el Código Penal Alemán regula la estafa de la siguiente forma en su art. 263: "Cualquiera que, con la intención de obtener una ventaja financiera ilícita para sí o para terceros, dañe el patrimonio de otro causando o manteniendo un error al fingir hechos falsos o suprimiendo hechos verdaderos, será castigado con pena de prisión por hasta cinco años…*".*

En este sentido, el tipo penal alemán presenta características similares al argentino, ya que el texto legal no hace mención de este acto de disposición al que venimos haciendo referencia. Es así que, desde la propia doctrina, se debieron hacer aclaraciones al respecto. En tal sentido, Kindhäuser afirma: "La estafa es un delito patrimonial en el que el titular padece un daño a consecuencia de una disposición defectuosa"[86].

Con respecto a los ejemplos legislativos traídos a colación, resulta evidente que la técnica adoptada por el sistema español resulta la más adecuada a la hora de subsumir los hechos que puedan ser catalogados dentro de la modalidad delictiva del *phishing defraudatorio* bajo la calificación legal de la estafa. Lo anterior, toda vez que, al suprimir el carácter de la patrimonialidad respecto del acto de disposición que debe realizar la víctima que es damnificada por esta clase de delitos, logra eliminar cualquier intento judicial de calificar esta clase de hechos como atípicos desde el punto de vista de la estafa -consumada o en grado de tentativa- y otras defraudaciones.

Ahora bien, incluso afirmando que la modalidad delictiva del *phishing defraudatorio* resulta atípica con relación al delito de estafa común por no compartir los criterios esbozados -*criterio amplio*-, resta analizarla a la luz de un último tipo penal.

E. Diferencias con el hurto -art. 162 del Código Penal-.

Tal como ocurre actualmente al intentar encontrar un encuadre legal adecuado para la modalidad delictiva del *phishing defraudatorio*, en caso de no contar con una figura acorde, y habiendo ya descartado la posible aplicación de los tipos penales contenidos en los arts. 172 y 173, inc. 16°, del Código Penal; restaría analizar si dicha modalidad delictiva puede ser evaluada bajo la luz de la figura del hurto simple del art.

[86] KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002. Pág. 159.

162 del Código Penal de la Nación. Ahora bien, resulta evidente que adoptar tal decisión, implicaría para el operador jurídico desentenderse de una serie de características que presenta esta modalidad delictiva que la asemejan más a una defraudación -como ser la existencia de un ardid o engaño, la incursión por parte de la víctima en un error, etc.-.

En primer término, un sector mayoritario de la doctrina[87] asegura que los delitos contra la propiedad como el hurto -o el robo- se diferencian de las defraudaciones por la circunstancia fáctica de la inmediatez entre la conducta desplegada por el sujeto activo y el daño a un tercero que implica el perjuicio patrimonial[88].

Dentro de la lógica señalada, se afirma que, mientras la disposición patrimonial en la estafa es un comportamiento que jurídicamente es imputado al titular del patrimonio, pero por el cual el autor es penalmente responsable a raíz del engaño -o ardid, abuso de confianza, etc.- causado en el marco de una relación interna con la víctima; en el hurto no sucede tal cosa[89]. Contrariamente, las acciones de desapoderamiento o sustracción propias de este delito pueden, desde un principio, ser imputadas al autor, debido a que este tipo penal presenta un elemento adicional que, comúnmente, es pasado por alto por parte de la doctrina. A saber: la inmediatez que caracteriza a la acción de sustracción y el consecuente daño a un tercero[90].

El elemento señalado en el párrafo precedente no es para nada menor debido a que la sustracción presupone una ruptura de la custodia[91], esto es, un traslado de la posesión contra la voluntad de quien, hasta entonces, era el titular de ésta. De hecho, se afirma que si el titular de la custodia es el propietario mismo o un tercero autorizado por ésta para la transferencia de la posesión: recién ahí entrará en consideración la estafa, debido a que el traspaso consentido de la custodia al autor tiene lugar a raíz del engaño o ardid del que fuera víctima[92].

Debido a la relevancia que tal supuesto presenta a los fines de este trabajo, vamos a dar un ejemplo concreto que ilustra lo anterior. Supongamos que una persona recibe un

[87] KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002. Pág. 159-160.
[88] Ibidem.
[89] Ibidem.
[90] Ibidem.
[91] KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002. Pág. 160-161.
[92] Ibidem.

llamado por parte de un desconocido que se hace pasar por el gerente de su banco y le informa, engañándolo, que se han detectado problemas en su cuenta y le solicita sus claves de acceso a *homebanking* para desviar sus fondos a una nueva cuenta (más segura) que será abierta a su nombre. Confiando en este desconocido que dice ser la máxima autoridad de la entidad bancaria, la persona le suministra dicha información y, conociendo las claves de la víctima, el autor desvía la totalidad de los fondos a una cuenta en el extranjero, de difícil rastreo, que es de su propiedad.

En el caso del *phishing defraudatorio* referido en el párrafo precedente, es dable notar que, por un lado, en lo que al resultado refiere, sí existe una sustracción en los mismos términos requeridos por la figura del hurto simple -art. 162 del CP-. Ahora bien, por otra parte, dicha sustracción sólo es posible con motivo de la presencia de aquel elemento referido por Kindhäuser y que sólo caracteriza a las defraudaciones, esto es*:* "...un comportamiento que jurídicamente es imputado al titular del patrimonio, pero por el cual el autor es penalmente responsable a raíz del engaño -o ardid, abuso de confianza, etc.- causado en el marco de una relación interna con la víctima"[93]. Lo anterior, toda vez que la sustracción sólo es posible debido al otorgamiento de claves -y demás datos de acceso, según el caso- efectuado por el titular del patrimonio que, ciertamente, actúa engañado.

Esta circunstancia ha traído consecuencias en el plano de la discusión jurídica nacional, en lo atinente a la correspondiente responsabilidad asumida por las entidades financieras[94] en casos de *phishing defraudatorio*. En tal sentido, en el pasado reciente, las instituciones bancarias se han expresado en el sentido de que no pueden ser responsables de las maniobras llevadas adelante por terceros ajenos a ellos; y que a todo evento la responsabilidad en el acaecimiento de este tipo de maniobras recae en el usuario financiero que, en muchos casos, desadvertidamente, facilita información sensible como contraseñas o *tokens* de seguridad a personas no autorizadas a tales fines[95].

En resumidas cuentas, el aporte de la víctima para esta clase de hechos no resulta una circunstancia únicamente discutida a la luz del análisis de la dogmática penal, sino

[93] KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002. Pág. 159-160
[94] BEKERMAN, Uriel y BASTUS, Guido. "Cibercriminalidad Financiera y 'Phishing' bancario: diagnóstico y herramientas de tutela judicial". En Sistema Penal e Informática. Editorial Hammurabi. Buenos Aires, 2022. Págs. 200-201.
[95] Ibidem.

que se ha extrapolado a diversos ámbitos de responsabilidad jurídica: por lo que su materialidad resulta evidente y rara vez discutida.

Esta realización nos lleva a descubrir una realidad que resulta ineludible: no es errado calificar una conducta de *phishing defraudatorio* bajo la calificación legal de hurto. El problema que esto encierra es la incompletitud en la que se verá envuelto dicho análisis, ya que ignora la naturaleza -defraudatoria- de dicha modalidad delictiva, al no contemplarse este aporte que la propia víctima realiza en el marco de la sustracción y que resulta un elemento ineludible que caracteriza a la modalidad delictiva descripta.

Estas conclusiones extraídas de diversos ámbitos doctrinarios sirven para reforzar la noción del absurdo que significaría la simplificación jurídica de contentarse con el tipo penal de hurto para calificar una conducta defraudatoria como lo es, a todas luces, el *phishing defraudatorio*. Ahora bien, para terminar de cerrar esta noción, resta analizar algunas de las conclusiones impartidas por la jurisprudencia local en torno a esta cuestión.

En dicha línea, ya hemos destacado que este trabajo se centra en el marco de lo ocurrido en la Ciudad Autónoma de Buenos Aires. En dicho sentido, en recientes fallos de la Cámara Nacional de Casación en lo Criminal y Correccional vinculados con cuestiones de delincuencia informática, se ha afirmado que la sustracción de dinero contenido en una cuenta bancaria no puede ser nunca calificado bajo la figura del art. 162 del Código Penal. Lo anterior, ya que es criterio de esa Cámara que el crédito bancario no se corresponde con el requisito de "cosa mueble" establecido por dicho tipo penal.

En dicha tesitura, la Sala II ha dicho "Pese a la evidencia de las dificultades que presenta, conforme a lo expuesto en el último considerando, afirmar que en el caso bajo análisis la conducta de la imputada consistió en el apoderamiento de una 'cosa mueble', de modo desconcertante, la cuestión no mereció ninguna clase de examen en la decisión recurrida. Así, el tribunal oral no expuso, siquiera mínimamente, las razones por las cuales una transferencia bancaria puede ser considerada como un acto de apoderamiento de una 'cosa mueble'.

Posiblemente, el motivo por el cual la subsunción efectuada en la sentencia no mereció ni la más mínima fundamentación por parte del a quo, radique en el entendimiento de que una transferencia bancaria implica el traslado de dinero físico, pues las monedas metálicas o el papel moneda, evidentemente, por reunir las características mencionadas anteriormente, pueden ser subsumidas sin mayores dificultades en el

concepto de ‘cosa mueble’. Esto se advierte con claridad si se analiza nuevamente el pasaje de la sentencia en el cual el magistrado sostuvo que la acusada se apoderó de ‘una cuantiosa suma de dinero’ que ‘estaba depositada en la cuenta de la cual era titular su exmarido’.

Sin embargo, esa caracterización del significado de una transferencia bancaria como la que se tuvo por acreditada en el caso no es correcta”[96].

En síntesis, y como ya se adelantó en el acápite anterior, no es posible afirmar que la modalidad delictiva del *phishing defraudatorio* encuentre acogida favorable en el tipo penal del hurto simple. Lo anterior, principalmente toda vez que, conforme el fallo transcripto *ut supra*, es criterio de la Cámara Nacional de Casación en lo Criminal y Correccional que las transferencias bancarias que son realizadas a través de medios informáticos (no dinero físico) no pueden ser consideradas como un “desapoderamiento de cosa mueble” (requisito del tipo objetivo para el delito de hurto simple). Por tal razón, el caso de *phishing defraudatorio* que definimos al inicio sería atípico a la luz de esta figura.

V. Dificultades para la investigación.

A. Ley de traspaso y conflicto de competencia territorial.

Ahora bien, habiendo descripto ya las principales problemáticas que el *phishing defraudatorio* encuentra en la actualidad a la hora de hallar una correcta calificación legal, debemos analizar otra de las dificultades que la persecución e investigación de tales delitos presenta. Al respecto, ya hemos comentado que este trabajo se centrará en lo que, actualmente, ocurre en el ámbito de la Ciudad Autónoma de Buenos Aires y los conflictos de competencia que se dan con respecto al fuero Nacional.

Como ya fue señalado es de público conocimiento que la Ley 26.702 de “Transferencia de Competencias Penales y Contravencionales de la Justicia Nacional Ordinaria a la Ciudad Autónoma de Buenos Aires” dispuso, en lo referente a “Delitos Vinculados a Competencia Pública Local”, en sus incisos “c)” y “d)”, el traspaso de una serie de tipos penales correspondientes a los delitos obrantes en el Capítulo IV del Título VI de nuestro código de fondo.

[96] CNCC. Causa Nro. 46.743/2017 -Reg. nro. 1190/2021-.

Sentado cuando precede, nos encontramos ante la siguiente cuestión en materia de competencia.

La estafa prevista en el art. 172 del Código Penal será de competencia nacional siempre y cuando no se dieren las causales previstas en el inciso "c)" del cuarto acápite de la Ley 26.702. Dicha disposición normativa refiere expresamente: "Estafa procesal acaecida en procesos judiciales tramitados ante los tribunales de la Ciudad Autónoma de Buenos Aires, (artículo 172, Código Penal)".

Contrariamente, y con relación defraudación informática tipificada en el art. 173, inc. 16, del Código Penal de la Nación, existen opiniones diversas en torno a qué organismo judicial deberá entender en materia de competencia.

Por un lado, existen posturas que afirman que la competencia con relación al delito de la defraudación informática, pese a no estar expresamente prevista por Ley 26.702, deberá igualmente corresponder al fuero de la Ciudad Autónoma de Buenos Aires. Lo anterior, toda vez que ese delito fue creado mediante la Ley 26.388. Es decir, fue creado con posterioridad a la sanción de la Ley 24.588 que "Garantiza los intereses del Estado Nacional en la Ciudad de Buenos Aires"[97].

A su vez, no huelga aclarar que la competencia para la investigación de las defraudaciones cometidas a través de medios informáticos vendrá determinada por la teoría de la ubicuidad, salvo que la complejidad de los hechos aconseje la aplicación del principio de funcionalidad[98].

En un sentido similar a la postura enunciada previamente, el Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires se ha pronunciado al respecto afirmando lo siguiente en un caso de defraudación mediante manipulación de un sistema informático -art. 173, inc. 16°, del CP-: "El Fiscal General adjunto, al tomar intervención, opinó que (…) 'la controversia se origina en torno a qué jurisdicción -local o nacional- le compete investigar la conducta penal denunciada' y, con relación a ello, entendió que 'la cuestión en debate presenta semejanzas con los resuelto por el Tribunal Superior de Justicia en expedientes n°6397/09 'NN s/ inf. art. 00' y n°7312 'Neves Canepa', del 21/12/10, en los que se afirmó que corresponde a los tribunales de la ciudad conocer en la investigación y

[97] Cámara Nacional de Apelaciones en lo Criminal y Correccional – Sala 7. Expte. CCC 17.507/2021/CA1 – "NN. Dte. O., C." Competencia. Defraudación Manipulación informática". La teoría de la ubicuidad sostiene que el hecho se considera cometido tanto en el lugar en donde se produjo la exteriorización de la voluntad criminal como en donde ocurrió el resultado, con lo cual quedan cubiertas ambas alternativas y se desvanece la posibilidad de la impunidad del hecho derivado de un conflicto negativo de competencia.
[98] Cámara Nacional de Apelaciones en lo Criminal y Correccional – Sala 5. Expte. CCC 32.778/2020/CA1 – "F.H.H.".

juzgamiento de delitos creados con posterioridad a la sanción de la Ley Nacional N°24.588' (…) Por los fundamentos expresados por el Fiscal General Adjunto, a los que remitimos en lo pertinente, por razones de brevedad y economía procesal, corresponde declarar la competencia del Juzgado en lo Penal, Contravencional y de Faltas n°31 para entender en la causa en la que se originó el presente incidente"[99].

Por otra parte, existe una postura emanada de la Cámara Nacional de Casación en lo Criminal y Correccional que afirma que, toda vez que la competencia relativa al tipo penal del art. 173, inc. 16°, no fue expresamente transferida a la justicia local mediante Ley 26.702: no corresponde su remisión al fuero de la ciudad[100].

Esta segunda postura no carece de argumento válidos. En este caso, se afirma, no sólo que no puede concluirse de la letra de la Ley 24.588 que todo delito tipificado con posterioridad a su promulgación resultará automáticamente competente para investigarlo el fuero Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires. Sino que también se reconoce, de la propia existencia del convenio surgido a raíz de la Ley 26.702, que la regla imperante en materia de competencia refiere precisamente a la promulgación de normas que ordenen dichas cuestiones[101]. Conforme esta lectura, se critica la interpretación que refiere que la defraudación informática es de competencia local por haber sido tipificada con posterioridad a la Ley 24.588 por ser flagrantemente contraria a la voluntad del legislador.

El criterio esbozado ha sido también replicado por la Procuración General de la Nación, al afirmarse que: "En tanto no existe una norma que expresamente transfiera la competencia de los tipos penales prescriptos en los incisos 15 y 16 del artículo 173 del Código Penal, ni se subsumen en la regla general prevista en el artículo 2 de la ley 26702, tal como lo sostuve y fue resuelto por la Corte Suprema en el precedente citado y sus antecedentes, cabe concluir que la competencia para intervenir en la investigación y el juzgamiento de los hechos ocurridos en la ciudad de Buenos Aires que se subsuman en el artículo 173, incisos 15 y 16, del Código Penal no integran la competencia de los tribunales locales"[102].

[99] Expte. N° TSJ 17891/2020-0 "NN, NN s/ 00 – Presunta comisión de delito (Art.173 inc. 16 CP) s/ Conflicto de competencia I".
[100] Cámara Nacional de Casación en lo Criminal y Correccional – Sala 2. Expte. CCC 38.624/2021/1/RH1. Reg. n°295/22. "N. N. s/ defraudación informática".
[101] Cámara Nacional de Casación en lo Criminal y Correccional – Sala 2. Expte. CCC 38.624/2021/1/RH1. Reg. n°295/22. "N. N. s/ defraudación informática".
[102] Resolución PGN N°38/2022.

En síntesis, la situación legal mencionada genera una serie de discrepancias respecto a qué fuero será el encargado de investigar y perseguir las maniobras delictivas de *phishing defraudatorio*.

En el ejercicio de la actividad judicial observada en los últimos años, es posible detectar no sólo la falta de un criterio uniforme con relación a qué se entiende por defraudación informática. Sino también falta de precisión respecto a definir y delimitar qué se entiende por *phishing*. Vale la pena recordar que no estamos ante una conducta poco frecuente. Conforme los datos y estadísticas reseñados al comienzo de este trabajo, el *phishing defraudatorio* es una de las maniobras delictivas de entidad patrimonial más comunes, no sólo en Argentina, sino a nivel mundial.

Para ilustrar brevemente lo señalado en el párrafo precedente, un reciente fallo de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, en el marco de la Causa Nro. 41.316/2021, determinó lo siguiente:

Se trató de un suceso mediante el cual se le imputó a "A. V. Paz" el haber tomado parte en una maniobra a través de la cual, mediante engaño, se lograron obtener los datos de acceso a homebanking de las cuentas que el presunto damnificado, "P. M. U." registraba en el Banco Ciudad; y, con ese uso no autorizado, mediante operaciones automáticas se realizaron un total de ocho transferencias por los montos de U$S10.000 y $919.000 en perjuicio de U.

Concretamente, el presunto damnificado denunció que el 30 de marzo del 2021, se contactó con el perfil de Banco Ciudad a través de la red social Facebook para realizar un reclamo y, minutos más tarde, una persona que se hizo pasar por empleado del banco se comunicó por medio del chat de la red social y le refirió que tenía que hacer una confirmación de sus cuentas para que las mismas no fueran bloqueadas.

Para ello, se le mostraron una serie de tarjetas de las cuales ella debía señalar cuáles le pertenecían, para luego finalizar la validación y recibir un código. Acto seguido, comenzó a recibir mensajes de texto en los que le informaban que se habían realizado dos transferencias desde su cuenta por un total de U$S10.000 y otras seis transferencias por un monto total de $919.000. Todas ellas realizadas a la cuenta registrada a nombre de la persona imputada.

Se calificó tal suceso como constitutivo del delito de defraudación informática conforme art. 173, inc. 16°, del Código Penal.

Ahora bien, y conforme lo señalado en este trabajo, resulta claro que el hecho investigado constituye una maniobra de *phishing defraudatorio* que, en su faz objetiva,

tiene más puntos de contacto con la estafa del art. 172 del código sustantivo que con el delito signado. Discrepancias como la remarcada surgen, claramente, a raíz de la falta de precisiones existentes en torno a qué características presenta la maniobra delictiva analizada.

Por otra parte, y en lo que a la investigación refiere, el *phishing defraudatorio* hereda gran parte de las discusiones relativas a los conflictos de competencia que imperan en torno a la defraudación informática. Se afirma lo anterior, toda vez que, al no existir una definición precisa de qué entendemos por dicha modalidad delictiva, es muy sencillo encontrar que los tribunales confunden este delito que acaba siendo subsumido bajo la calificación legal del art. 173, inc. 16, del Código Penal -como hemos visto en el ejemplo transcripto en los párrafos anteriores-.

En este sentido, se torna necesario remarcar que la modalidad delictiva del *phishing* requiere de una investigación rápida y eficaz a los fines de evitar la impunidad del delito. En dicha inteligencia, las dilaciones y demoras que resultan producto de numerosas contiendas de competencia atentan claramente contra la correcta investigación y persecución de tal modalidad delictiva.

B. Dificultades que se presentan a la hora de investigar en la red.

Ahora bien, y ya sólo a título de mención, se analizarán algunas de las dificultades que se presentan a la hora de investigar en internet y que afectan, particularmente, a la maniobra del *phishing*. Lo anterior, con el objeto de que dichas dificultades sean tenidas en cuenta a la hora de llevar a cabo las correspondientes modificaciones legislativas que sí contengan a la modalidad delictiva a la que se viene haciendo referencia.

El modo de comisión de los delitos informáticos -con los que el *phishing* y el *phishing defraudatorio* guardarían una relación de especificidad en caso de contar con tipos penales autónomos como ocurre en otros países- les otorga ciertas particularidades que los diferencian instrumentalmente del resto: haciendo que su investigación (policial y judicial) resulte mucho más compleja que en otros casos. Además, el medio a través del cual se consuman estos ilícitos permite una gran variedad de posibilidades (que incluyen amenazas, violación a la intimidad, relevación de secretos, corrupción de menores, exhibicionismo, etc.).

Esas peculiares características son -utilizando como referencia en forma parcial a Daniel Hargain[103]- las siguientes:

1. En primer lugar, la potencialidad del alcance de las conductas desarrolladas a través de internet, que no se circunscriben a un ámbito geográfico determinado, sino que pueden esparcirse a través de toda la web, que hace que estos crímenes no reconozcan fronteras territoriales. En su mayoría, se trata de delitos trasnacionales, como las redes de pedofilia o de lavado de dinero[104].

2. En segundo lugar, el anonimato. En muchísimas ocasiones resulta imposible o muy difícil identificar a quién está detrás de una computadora, desde dónde se envía un mensaje a través de la red o al responsable de una página web[105].

3. Y, en tercer lugar, la complejidad técnica del tema y el dinamismo vertiginoso con que evoluciona. El punto más dramático, a propio entender de Hargain, para la persecución penal de los mismos; y que ya hemos venido advirtiendo en el transcurso de este trabajo[106].

i: Ausencia de fronteras para delimitar la investigación.

La posibilidad tecnológica de las comunicaciones a distancia a través de las redes concibe que el delincuente se encuentre físicamente alejado (incluso por medio de varios países) de la víctima. Ya fue señalado que esta característica es de relevancia debido a que, en el caso del cibercrimen, las bandas organizadas suelen realizar los delitos desde determinados países cuyas características propias -complicaciones de idioma, falta de legislación en la materia, falta de cooperación internacional para la justicia, entre otros- hacen que las investigaciones sean de alto nivel de complejidad, con un nivel de eficacia prácticamente nulo[107].

La internacionalidad, como propiedad de los delitos informáticos, implica que los mismos no encuentran barreras jurisdiccionales para llevarse a cabo. Es decir, y a modo de ejemplo, es técnicamente posible estar conectado a una red en Argentina, pasar por un

[103] HARGAIN, Daniel. "*Incidencia del comercio electrónico en el ámbito jurídico: planteo general*". En Comercio electrónico. Análisis jurídico multidisciplinario – Euro Editores SRL. Buenos Aires 2003. Págs. 22-23.
[104] Ibidem.
[105] Ibidem.
[106] Ibidem.
[107] TEMPERINI, Marcelo. "*Delitos informáticas y cibercrimen: alcances, conceptos y características*". En suplemento especial, Erreius. Buenos Aires 2018. Pág. 62.

router[108] conectado en Rusia, utilizar una *botnet*[109] de computadoras en Colombia y finalmente atacar un sistema en Argentina. Por más complejo que pueda parecer en el enunciado, a nivel práctico es de relativa facilidad, siempre que se cuente con un mínimo de conocimientos técnicos.

Todo ello postula el claro desafío de coordinar distintos ámbitos de colaboración internacional. Con relación a este último aspecto, el Convenio de Cibercriminalidad de Budapest, del que ya hemos hablado anteriormente, ha sido el instrumento internacional más importante en la materia porque apuntó a tener dentro de los Estados firmantes un mínimo de coordinación en el ámbito penal material, y un potente marco de cooperación internacional (procesal penal) para la investigación de estos casos.

Como ya hemos señalado, Argentina es miembro de este Convenio que, a través de la Ley 27.411, ratificó su adhesión, aunque con algunas reservas. En este sentido, nuestro país tiene tareas pendientes en distintos aspectos que debe cumplimentar para formar parte de dicho grupo, tanto en materia de derecho sustantivo -que es parte del objeto de este trabajo- como de derecho procesal penal.

Más allá de la necesidad de cooperación internacional, se considera importante marcar la necesidad de un previo marco de cooperación nacional en Argentina. En la actualidad, se pueden observar diferentes realidades en nuestro país que dependen del grado de desarrollo o fortaleza económica de cada Provincia en particular. A modo de ejemplo, podría mencionarse que las víctimas de la Ciudad Autónoma de Buenos Aires poseen la posibilidad de denuncia ante la División de Delitos Tecnológicos de la Policía Federal Argentina, ante la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas del Ministerio Público Fiscal de la Ciudad -UFEDyCI-, o ante la Unidad Fiscal Especializada en Ciberdelincuencia -UFECI-. Todo lo cual, como ya hemos señalado, redunda en diversas dificultades en materia de competencia: pero eso es otra cuestión.

Dada la heterogeneidad de situaciones hacia el interior de nuestro país, se ha propuesto considerar la necesidad de generar una "Red Nacional de Cooperación en materia de Delitos Informáticos", para que aquellas Provincias (Catamarca, Jujuy, Entre Ríos, Santa Fe, etc.) que aún no poseen una estructura armada en la materia puedan acceder a los avances y experiencias de otras con mayor desarrollo en el área (tales como

[108] Un *router* o enrutador es un dispositivo que proporciona conectividad a nivel de red.
[109] Una *botnet* es una red de computadoras "zombies", es decir que han sido previamente infectadas y que permiten que quien tenga su control pueda utilizarlas como armas para distintos tipos de ataques.

la Ciudad Autónoma de Buenos Aires y Córdoba). Y de este modo posibilitar la creación de canales ágiles de cooperación para los casos que requieran colaboración interjurisdiccional[110].

ii. Anonimato.

La segunda dificultad que se presenta a la hora de investigar el *phishing* es, precisamente, el anonimato del cual se valen los sujetos que llevan a cabo tales conductas.

En esa línea, existe una percepción general por parte de la mayoría de la población de que las tecnologías son neutras y su valoración dependerá pura y exclusivamente de lo que el hombre en sí decida hacer con ellas. En el caso de la comisión de los delitos informáticos, las distintas técnicas de anonimato existentes -en el caso de que sean utilizadas- llevan al instructor/investigador a enfrentarse con un complejo desafío al momento de intentar determinar al autor de dichas maniobras delictivas[111].

Ahora bien, es sencillo notar que, así como no es posible afirmar que una tecnología sea 100% segura, tampoco lo es afirmar que una tecnología ofrezca un 100% de anonimidad. Por eso, desde una perspectiva técnico-jurídica, se considera más adecuado hablar de niveles de anonimato que, dependiendo del tipo de tecnología utilizada, implicarán un mayor desafío para el investigador. A modo de ejemplo, no implica un mismo nivel de anonimato el de un delito cometido desde un wifi público (un bajo nivel) que el de un delito cometidos desde la red TOR -una de las puertas de entrada para la *Deep web*-, en el cual existe un encadenamiento de proxys anónimos que complejiza mucho más la investigación. Y ni hablar si, a lo anterior, agregamos el factor de dificultad que puede adicionar la utilización de un servicio de VPN -que hoy en día es ofrecido gratuitamente por numerosas compañías de seguridad digital y antivirus-.

No obstante, vale la pena remarcar que la *Deep web* es un espacio virtual que existe en la actualidad y que es cada vez más accesible para los usuarios, y que posee determinadas características que es necesario considerar si se quiere hacer un estudio completo sobre los delitos informáticos[112]. Esta *Deep web* (también llamada *Internet profunda* o *Internet oculta*) no es más que una parte de la red de Internet en la cual los

[110] TEMPERINI, Marcelo. "Delitos informáticas y cibercrimen: alcances, conceptos y características". En suplemento especial, Erreius. Buenos Aires 2018. Pág. 63.
[111] TEMPERINI, Marcelo. "Delitos informáticas y cibercrimen: alcances, conceptos y características". En suplemento especial, Erreius. Buenos Aires 2018. Pág. 64.
[112] TEMPERINI, Marcelo. "Deep web, anonimato y cibercrimen". VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016).

contenidos no son indexados por los motores de búsquedas tradicionales (Google, Yahoo, Bing, etc.). Por ello, y en contraste con la *Deep web*, a Internet como lo conocemos se lo conoce también como "Internet superficial".

Los contenidos pueden no ser indexados por distintas razonas, entre las que encontraremos: páginas web dinámicas, sitios bloqueados (por un CAPTCHA, por ejemplo), sitios privados (acceso solo con "logueo" previo), sitios con contenidos que no son HTML, así como redes de acceso limitado (por ejemplo, a determinados protocolos de accesos). Dentro de estos últimos, de contenidos que solo son accesibles a través de un determinado software o protocolo específico, podemos encontrar al Proyecto TOR, una de las herramientas más conocidas, que construye un circuito de conexiones cifradas a través de repetidores en la red, donde el circuito se extiende un salto a la vez. Cada nodo a lo largo del camino conoce únicamente el nodo que le proporciona los datos y retransmite los que les entrega. De esta forma un nodo, de forma individual, nunca conoce el recorrido completo que ha tomado un paquete de datos. El cliente negocia un paquete separado de claves de cifrado para cada tramo a lo largo del circuito, asegurando que la información circulante entre los nodos no pueda ser rastreada.

Para ilustrar las dificultades que la *Deep web* presenta a la hora de llevar a cabo investigaciones en materia de ciberdelincuencia, se va a citar un importante caso que tuvo lugar en el año 2014. En aquel tiempo, se llevó a cabo una operación ONYMOUS que sirve de ejemplo de que a través de la cooperación internacional y el trabajo serio de organismos dedicados a combatir el crimen organizado internacional. La misma ha sido llevada a cabo en siete (7) países, se han intervenido cuentas de Bitcoin por valor de un (1) millón de dólares, ciento ochenta mil euros (180.000€) en efectivo y distintos tipos de estupefacientes. Este operativo requirió la participación de dieciocho (18) países coordinados estrechamente por Europol, Eurojust y el Departamento de Justicia de los Estados Unidos, y ha permitido detener de forma simultánea a diecisiete (17) personas -de 8 de Reino Unido, 3 de Estados Unidos, 1 de España, 1 de Hungría, 2 en Suecia, 1 en Suiza y 1 de Irlanda- que controlaban los mercados clandestinos con mayor volumen de negocio en la red TOR, reiteramos, caracterizada por el anonimato que proporciona a sus usuarios[113].

Dicha operación ha evidenciado que a través de la cooperación internacional se puede investigar y/o determinar responsables de la infraestructura criminal que utiliza la

[113] TEMPERINI, Marcelo. "Deep web, anonimato y cibercrimen". VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016).

delincuencia organizada en internet, sobre la que se había generado cierta sensación de impunidad por el anonimato que proporcionan estos servicios ocultos dentro de la red[114].

A nivel local, un operativo como el descripto en los párrafos anteriores, requeriría de la cooperación y coordinación de los distintos países que integran el MERCOSUR. A la fecha, no existen tratados de cooperación internacional que permitan llevar adelante tales tareas investigativas.

VI. Postura y conclusiones.

A. Legislación comparada y casos de relevancia mundial.

Ahora bien, se torna imperioso también remarcar que, en otras legislaciones, como la norteamericana, la penalización de la obtención ilegal de datos personales como forma de detener el robo de identidad o *identity theft* se legisló en varias oportunidades. Tal es así, que la Ley de Modernización Bancaria se aprobó en noviembre de 1999 y contiene todo un conjunto de normas federales sobre privacidad bancaria. Ella contiene un título denominado The Financial Privacy Law, con dos subtítulos: el A, relativo a nuevas obligaciones sustantivas relacionadas con la revelación de datos personales por parte de entidades financieras a terceras partes no afiliadas, y un B, que establece nuevos delitos federales que penalizan la adquisición fraudulenta de información sobre clientes bancarios.

El subtítulo B de la ley fue una de las respuestas del Congreso a los escándalos ocurridos en las últimas décadas con los llamados *information brokers*, quienes de forma desleal y con pretextos y escusas falsas, procuraban la obtención de datos personales y económicos de clientes de bancos para venderlos a terceros o cometer delitos, el más común de los cuales era el robo de identidad[115]. Este escenario es muy similar a lo que sucede, hoy en día, con el *phishing* en Argentina. En el caso de Estados Unidos de América, al entenderse que tales delitos perjudicaban tanto a clientes como a bancos por igual, se decidió criminalizar la obtención de datos personales a través de dicha modalidad

[114] TEMPERINI, Marcelo. "Deep web, anonimato y cibercrimen". VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016).
[115] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 167.

delictiva: supuesto que coincide con el fraude mediante el empleo de *phishing* analizado en este trabajo.

A su vez, en la legislación norteamericana existen fuertes regulaciones en torno al acceso no autorizado a sistemas informáticos. En dicho sentido, el Acta de Fraude y Abuso Informático (*Computer Fraud and Abuse Act*) es de competencia federal y la doctrina especializada en tal cuestión, sostiene que no es tarea sencilla establecer en qué supuestos existe acceso autorizado a un sistema informático y en cuáles no[116]. Analizando este ejemplo con relación al *phishing*, podría suponer graves inconvenientes interpretativos a la hora de investigar aquellos delitos que hubieren quedado en grado de connato, ya que una parte importante de la discusión giraría en torno al potencial peligro de la maniobra desde la perspectiva de un acceso obtenido de forma fraudulenta. En tal sentido, vale la pena traer a colación un reciente reportaje de la BBC que definió al *phishing* como *el talón de Aquiles de la economía norteamericana* debido a que, con motivo de tales conductas, varias empresas han registrado pérdidas millonarias[117]. En el último tiempo, se ha recrudecido las medidas por parte del Departamento de Justicia Norteamericano debido a que se ha registrado la existencia de mecanismos que, mediante Inteligencia Artificial, permiten imitar voces a los fines de perfeccionar dichas maniobras[118].

En el Reino Unido, la sección 55° de la *Data Protection Act* penaliza a quien obtenga, revele o procure la facilitación de datos personales sin el consentimiento del responsable del tratamiento. Desde la perspectiva del *phishing*, esta forma de legislar dichas conductas tendría el defecto de remitirse al consentimiento brindado por parte del responsable del tratamiento y no del titular de los datos.

En España, por su parte, la solución se dio con el nuevo Código Penal del 1995, ya que en éste se agregó al delito tradicional de estafa (art. 248 BOE), un artículo que incluye a la defraudación informática (art. 249, inc. 2, "a)" BOE). De esta forma, se superaron los inconvenientes señalados por la doctrina. Tal es así que, en la legislación española, tanto el *phishing defraudatorio* como la defraudación informática quedan claramente delimitados el uno respecto del otro.

[116] KERR, Orin S. "Norms of Computer Trespass". Columbia Law Review, Vol 116:1143, 2016.
[117] https://www.bbc.com/mundo/noticias-63494702
[118] https://panampost.com/oriana-rivas/2024/03/07/eeuu-sentencias-delitos-con-inteligencia-artificial/

En el caso del art. 248, como ya se advirtió, se sorteó el inconveniente del elemento constitutivo de la disposición que debe realizar la víctima; resultando este artículo de sencilla aplicación con relación a todos los casos de *phishing defraudatorio*.

Por otra parte, el art. 249, inc. 2, "a)", se aplicará en los casos en los cuales el engaño recaiga sobre una máquina en lugar de una persona.

En América Latina, en Puerto Rico, tanto la estafa como la defraudación informática se encuentra reguladas en los arts. 202 y 203 del Código Penal, respectivamente. La letra de dichos artículos reza lo siguiente:

"Artículo 202. — Fraude. (33 L.P.R.A. § 5272) Será sancionada con pena de reclusión por un término fijo de ocho (8) años, toda persona que fraudulentamente con el propósito de defraudar: (a) Induzca a otra a realizar actos u omisiones que afecten derechos o intereses patrimoniales sobre bienes inmuebles o bienes muebles de esa persona, del Estado o de un tercero, en perjuicio de éstos; o (b) Realice actos u omisiones que priven a otra persona o afecten los derechos o intereses patrimoniales sobre bienes inmuebles o bienes muebles para perjuicio de ésta, del Estado o de un tercero. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000). El tribunal también podrá imponer la pena de restitución.

Artículo 203. — Fraude por medio informático. (33 L.P.R.A. § 5273) Toda persona que con el propósito de defraudar y mediante cualquier manipulación informática consiga la transferencia no consentida de cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionada con pena de reclusión por un término fijo de ocho (8) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000). El tribunal también podrá imponer la pena de restitución".

En este caso, se puede observar que subsisten los problemas interpretativos que presenta nuestra legislación con respecto al *phishing defraudatorio*. Se afirma lo anterior, toda vez que dicha modalidad delictiva no se encuentra contenida específicamente en el fraude informático; pero tampoco, al ser tan abarcativo el tipo penal del fraude, resulta sencillamente aplicable con respecto a este tipo penal.

Continuando en América Latina, un caso interesante para analizar desde el punto de vista legislativo es el de Colombia. Ese país reformó su Código Penal en el año 2009

y se agregó un nuevo artículo que dispone lo siguiente: "Art. 269G: 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 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito*".*

Este tipo penal resulta muy llamativo por tres (3) cuestiones. La primera de ellas es que esta norma incluye, en su modalidad comisiva, al *web spoofing*, modalidad delictiva que implica la imitación de un determinado sitio web a los fines de llevar a cabo maniobras defraudatorias. La segunda, tiene que ver con la curiosa circunstancia relativa a que, si bien se reconoce la diferencia técnica existente entre el conocimiento -como *dominabilidad* del suceso- requerido para clonar un sitio web (el *web spoofing*, básicamente), y la dificultad que implica modificar una IP y/o un sistema de resolución de nombres de dominio: ambas modalidades comisivas importan el mismo monto de pena según la letra del tipo penal transcripto.

La tercera, y más llamativa, radica en la circunstancia de que, si bien esta norma se adecúa a la mayoría de las formas comisivas que caracterizan al *phishing*; por una mera cuestión de redacción del tipo penal, no incluye a aquellas conductas que se valen de métodos de ingeniería social que, como ya sabemos, son las más utilizadas.

Asimismo, es válido remarcar que muchos países carecen de un tipo penal como el art. 269G del Código Penal de Colombia que penalice al *web spoofing*[119]: y nuestro país es uno de ellos.

[119] El *web spoofing* consiste en la suplantación de una página web real por otra falsa con el fin de realizar una acción fraudulenta

B. Últimas impresiones.

Habiendo concluido con el estudio de las normas involucradas en el ámbito del presente trabajo y de los casos relevantes a tales efectos, se torna imperioso reseñar cuáles serán las conclusiones que permitirán resumir los principales argumentos de este trabajo.

En dicho sentido, el razonamiento más evidente que se pretende evidenciar radica en la circunstancia de que la defraudación mediante el empleo de *phishing* parecería encontrar su arraigo más firme en el art. 172 del Código Penal, conforme el criterio impartido por el Prof. Edgardo Donna.

En tal sentido, el *phishing defraudatorio* que fue señalado como aquella maniobra de naturaleza patrimonial que más denuncias o reportes presenta en la actualidad según recientes informes[120]: podría ser calificado bajo los estándares de dicha norma penal. Ahora bien, esto continúa presentando algunos inconvenientes.

¿Y por qué se afirma lo anterior? Veamos.

Por un lado, y como ya fue analizado, se consideran elementos estructurales del tipo objetivo de la estafa, los siguientes: **1)** la existencia de un ardid o engaño, **2)** la incurrencia en un error por parte del sujeto pasivo, **3)** la realización de un acto de disposición patrimonial por parte de la víctima y, **4)** el acaecimiento de un perjuicio económico.

En tal sentido, en el caso del *phishing defraudatorio*, se ha concluido que la víctima no realiza un acto de disposición patrimonial en sentido estricto (por ejemplo: al facilitar sus claves personales no estaría efectuando un acto de disposición patrimonial). Por el contrario, el sujeto pasivo suministra al autor una serie de datos vinculados a sus cuentas informáticas destinadas a salvaguardar su patrimonio -como puede ser *homebanking*, plataformas de pago, compraventa, etc.-. Datos que el sujeto activo utiliza para procurar una ventaja patrimonial en favor de sí o de un tercero. Todo lo cual, llevaría al interprete a la obligación de adoptar el *criterio amplio* esbozado previamente.

En dicha inteligencia, la tipificación del delito de la estafa común siguiendo la técnica legislativa vislumbrada en el Código Penal Español, lograría evitar dicha dificultad.

Por otra parte, conforme los lineamientos detallados en materia de Teoría del Delito, dicha afirmación presenta algunos inconvenientes en aquellos casos en los cuales la maniobra permanezca en grado de connato. Lo anterior, toda vez que habría que

[120] UFECI – Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Buenos Aires, 2021. Pág. 18.

dilucidar si, en tal caso, el *phishing* opera como acto preparatorio o acto ejecutivo de tentativa. En caso de que se determine que se trató de un mero acto preparatorio, amén de no verificarse la puesta en peligro y la inmediatez temporal entre: i) la *pesca* de datos mediante técnicas de ingeniería social y, ii) la puesta en peligro con respecto al bien jurídico patrimonial en cuestión; la conducta en cuestión devendrá en atípica.

Ahora bien, y en este estadío del análisis del objeto de estudio que involucra a este trabajo, a lo enunciado en el acápite "IV" se puede adicionar lo observado en otras legislaciones con relación a la modalidad delictiva del *phishing*. En la mayor parte de ellas, y en particular en el caso de la norteamericana, el suministro de claves no es entendido como un acto de disposición patrimonial: sino como una lesión a la propia privacidad y a la libertad de la persona afectada. De ahí que, en muchos ordenamientos jurídicos en los que sí está legislado, se sostenga que el fraude mediante el empleo de *phishing* resulta un delito autónomo pluriofensivo[121] y no meramente patrimonial. A su vez, en el caso de la legislación norteamericana, se ha visto que existen figuras de peligro que criminalizan a la modalidad delictiva del *phishing*: evitando así la posibilidad de incurrir en conductas que resultaren atípicas como ocurre en nuestro sistema.

Por otra parte, y con respecto a la defraudación informática del art. 173 inc. 16 del Código Penal, se remarcó que existe un elemento del tipo objetivo que se encuentra ausente en los casos de *phishing* que fueron analizados. Esto es, el empleo de "cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos". Lo anterior, toda vez que hemos afirmado que el *phisher* no requiere del malfuncionamiento de un sistema informático para lograr su cometido.

Todo ello, redunda necesariamente en la obligación jurídica de reconocer que el *phishing*, como modalidad comisiva, no coincide de forma íntegra con los tipos penales analizados.

Por tales motivos, ha de tornarse necesario analizar la posibilidad de que sea un texto legal independiente el que contemple dicha modalidad delictiva.

Por último, estamos en condiciones de poner de relieve las deficiencias que presentan varias de las definiciones existentes acerca del *phishing*: tanto la expuesta al inicio de este trabajo, como aquellas que bogan por la presencia de una *ultrafinalidad* relativa a la suplantación de identidad.

[121] PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016. Pág. 166.

La importancia de contar con una definición precisa con respecto a qué modalidad/es delictiva/s deberían contener al *phishing* resulta evidente; no sólo para mejorar y facilitar la labor jurídica con relación al juzgamiento e interpretación de este tipo de conductas. Sino también para evitar contiendas de competencia innecesarias que lo único que logran es generar dilaciones en una investigación que, por el contrario, debe ser rápida y expedita a los fines de evitar la impunidad.

B. Postura.

De lo expuesto, se puede deducir que, en materia de derecho sustantivo, una de las principales variables que el legislador puede controlar a los fines de garantizar y facilitar una rápida y expedita investigación en materia de *phishing*: es dotar a esta modalidad delictiva de un tipo penal autónomo que la exima de las dificultades interpretativas que exponen las figuras penales analizadas en este trabajo -arts. 162, 172 y 173, inc. 16, CP-.

Resulta evidente que, si bien es cierto que del propio análisis jurisprudencial se desprende que la modalidad delictiva analizada hasta ahora presenta mayores coincidencias con el tipo penal de la estafa; esta calificación -en su faz objetiva- no se condice exactamente con el *phishing*. Circunstancia que conducirá, invariablemente, y mientras no se produzcan las modificaciones legislativas pertinentes, a conflictos interpretativos en el marco del derecho sustantivo y, consecuentemente, a investigaciones que no avanzarán por entenderse que se trataría de una conducta atípica.

A lo anterior, debe adicionare las complejidades que el *phishing* ha presentado en los últimos tiempos debido a la inserción de la Inteligencia Artificial en el ámbito de la informática. Lo anterior, le ha permitido a los *phishers* perfeccionar sus maniobras mediante el empleo de herramientas que permiten la modificación de la voz, entre otras cuestiones.

¿Y cómo se puede legislar dicha conducta? Conforme lo reseñado en este trabajo, un ejemplo de correcta tipificación sería el caso de España: si el objetivo es ampliar a la estafa común para que la misma pueda contener al *phishing* evitando problemas interpretativos. Ahora bien, si la finalidad fuera la de aceptar a esta conducta como un delito pluriofensivo y así dotarla de un tipo penal autónomo, *a priori*, una solución eficaz en dicho sentido podría ser la adoptada por el Estado de Minnesota de los Estados Unidos de América: legislar al *phishing* como un delito autónomo de peligro concreto. Lo

anterior, incluyendo en su formulación una cláusula relativa a salvaguardar posibles problemas interpretativos en torno a la concurrencia aparente de tal delito con otras figuras, como sucede con el tipo penal del art. 183 del Código Penal, al referirse "...siempre que el hecho no constituya otro delito más severamente penado".

Esta última solución podría llevar, como correlato, a la tipificación autónoma del *phishing defraudatorio* como delito doloso de resultado en un nuevo acápite dentro del art. 173 del Código Penal, es decir, como un nuevo supuesto de defraudación que tenga al *phishing* como modalidad comisiva.

Por último, y como ya fue señalado, otra ventaja que acarrearía esto en el seno de lo que ocurre en el ámbito de la Ciudad Autónoma de Buenos Aires -al menos en el futuro inmediato-; sería también la de evitar las dilaciones propias que se generan con motivo de innecesarias contiendas de competencia en el marco de una investigación.

Ahora bien, y amén de lo señalado hasta ahora, no existen a la vista proyectos de ley y/o modificaciones legislativas que pretendan resolver esta cuestión.

Bibliografía:

- ANTON ONECA, José. "Las estafas y otros engaños, en el Código penal y en la jurisprudencia". Anuario de Derecho Penal y Ciencias Penales (1958).
- BEKERMAN, Uriel y BASTUS, Guido. "Cibercriminalidad Financiera y 'Phishing' bancario: diagnóstico y herramientas de tutela judicial". En Sistema Penal e Informática. Editorial Hammurabi. Buenos Aires, 2022.
- CONDE-PUMPIDO FERREIRO, Cándido. "Estafas". Tirant Lo Blanch. Valencia 1997.
- CREUS, Carlos. "Derecho Penal. Parte Especial. Tomo I – 6ta edición actualizada y ampliada". Editorial Astrea. Buenos Aires, 1997
- DONNA, Edgardo Alberto. "Derecho Penal. Parte Especial. Tomo II-B". Rubinzal-Culzoni Editores. Buenos Aires 2001.
- HARGAIN, Daniel. "Incidencia del comercio electrónico en el ámbito jurídico: planteo general". En Comercio electrónico. Análisis jurídico multidisciplinario – Euro Editores SRL. Buenos Aires 2003.
- HILGENDORF, Eric y VALERIUS, Brian. "Derecho Penal. Parte General". Editorial Ad-Hoc. Primera Edición. Traducción de la 2da edición alemana. Buenos Aires, marzo del 2017.
- KERR, Orin S. "Norms of Computer Trespass". Columbia Law Review, Vol 116:1143, 2016.
- KINDHÄUSER, Urs. "La estafa por medio de computadoras: ¿una estafa?". Estudios de Derecho Penal Patrimonial, Lima, Instituto Peruano de Ciencias Penales/Editora Jurídica Grijley, 2002
- MIR PUIG, Santiago. "Derecho Penal. Parte General". 10ª ed. Editorial Reppertor. Barcelona 2016.
- MORENO, Rodolfo. "El Código Penal y sus Antecedentes". H.A. Tomassi Editor. Buenos Aires 1992.
- PALAZZI, Pablo. "Los delitos informáticos en el Código Penal". Abeledo-Perrot Editores. Buenos Aires 2016.
- PEDRAZZI, Cesare. "Inganno ed errore nei delitti contro il patrimonio". Dot. A. Giuffré Editore. Milano 1955

- RODRÍGUEZ, Pedro. “Casos especiales de defraudación. Código Penal Comentado de Acceso Libre” en Revista de Derecho Penal, Asociación Pensamiento Penal.
- ROIBÓN, María M. “Reflexiones sobre el acceso ilegítimo a un sistema o dato informático”. En Revista Erreius, “Cibercrimen y Delitos informáticos”. Buenos Aires, 2018.
- SOLER, Sebastián. “Derecho Penal Argentino. Tomo IV”. Tipográfica Editora Argentina. Buenos Aires 1992.
- TAZZA, Alejandro. “Código Penal de la Nación Argentina. Comentado. Tomo II”. Rubinzal-Culzoni Editores. Santa Fe 2018.
- TEMPERINI, Marcelo. “Deep web, anonimato y cibercrimen”. VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016).
- UFECI – Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020. Buenos Aires, 2021.
- WELZEL, Hans. “Derecho Penal Alemán. Parte General”. Trad. Juan BUSTOS RAMÍREZ y Sergio YAÑÉZ PERES). 11ª ed. (4.ª ed. en español). Editorial Jurídica de Chile, Santiago, 1970.
- ZAFFARONI, Raúl Eugenio; SLOKAR, Alejandro y; ALAGIA, Alejandro. “Derecho Penal. Parte General”. Editorial Ediar. Buenos Aires 2002.
- ZAFFARONI, Raúl Eugenio y; BAIGÚN, David. “Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial. Tomo VII”. Editorial Hammurabi.