El fraude informático mediante ingeniería social: una aproximación a su encuadramiento legal.

Mag. Abog. Roberto Javier Pizzo[1]

Esp. Abog. Sabrina Lamperti[2]

Sumario: 1. Introducción - 2. Defraudaciones informáticas y estafas concretadas mediante técnicas y sistemas informáticos. - 3. La defraudación informática en particular – 4. Conducta típica – 5. Modalidades de fraudes informáticos – 6. Técnicas de ingeniería social – 7. Conclusiones

1. Introducción:

En el contexto de la emergencia sanitaria atravesada por el país y el Aislamiento Social, Preventivo y Obligatorio dispuesto mediante decreto de necesidad y urgencia 297/2020 y su plexo normativo complementario, se produjo un notorio crecimiento de las investigaciones penales por defraudaciones informáticas, en los que se observan diversas y renovadas modalidades que, al amparo del uso de las tecnologías, amenazan y perjudican el patrimonio de las víctimas. Dentro de la heterogeneidad de conductas ejecutadas con herramientas digitales, nos interesa destacar aquellas cuyas fenomenologías despiertan disparidad de opiniones con respecto a su encuadramiento legal. Nos referimos de manera particular a los fraudes cometidos con el uso de técnicas de ingeniería social.

Con relación a éstos, cabe decir que un sector de la doctrina considera que, cuando el autor obtiene con cierta habilidad las claves de acceso a un sistema informático -ya sea telefónicamente o mediante *phishing*-, la maniobra no subsume en la figura del fraude informático, sino en la estafa. Entienden en ese sentido que aquí no habría manipulación informática destinada a alterar el sistema, sino un accionar sobre el punto mas débil de la

1 Abogado (UNMDP), Magister en Derecho y Magistratura Judicial (Facultad de Derecho de la Universidad Austral). Fiscal titular de la Unidad Funcional de Instrucción y Juicio N.º 10 de Delitos Económicos, Departamento Judicial Mar del Plata.

2 Abogada (UNMDP), Especialista en Criminalidad Económica (Universidad Castilla-La Mancha). Instructora Judicial de la Unidad Funcional de Instrucción y Juicio N.º 10 de Delitos Económicos, Departamento Judicial Mar del Plata. Integrante del equipo de referentes digitales del Ministerio Público Fiscal de la Procuración General de la Provincia de Buenos Aires. Docente de Derecho Informático e investigadora académica del Laboratorio de I+D en Informática Forense.

cadena de seguridad informática, que es el factor humano[3].

Sin embargo, creemos que tal interpretación enfrenta serias dificultades dogmáticas, desde que la *praxis* diaria demuestra que en estas modalidades se encuentran ausentes elementos indispensables que estructuran el tipo objetivo previsto por art. 172 del Código Penal, y que, en realidad, nos encontramos frente a conductas delictivas que constituyen defraudaciones informáticas.

Por ello, resulta interesante abordar la problemática desde aspectos prácticos y efectuar un análisis somero de los casos de ingeniería social que se observan de manera frecuente, en procura de contribuir a una interpretación uniforme acerca de su correcta calificación legal.

2. Defraudaciones informáticas y estafas concretadas mediante técnicas y sistemas informáticos.

En principio, es importante señalar que existen numerosas modalidades cometidas con la utilización de herramientas digitales que no configuran fraudes informáticos sino estafas[4], dado que en sus plataformas fácticas se advierte la presencia de los elementos básicos de dicha figura; esto es: el ardid (o engaño), el error y la disposición patrimonial; los que se encuentran vinculados por una relación de causalidad, de modo tal que es el ardid desplegado por el sujeto activo el que ha generado error en la victima y ésta, en base a dicho error, quien realiza una disposición patrimonial perjudicial[5].

Sabido es que los requisitos del tipo objetivo mencionados, no se dan necesariamente en los fraudes generados con abusos de confianza o de situación, que pueden cometerse cuando el autor aprovecha situaciones que facilitan o permiten consumar el perjuicio patrimonial.

Pueden citarse como casos de estafas tradicionales cometidas con el uso de entornos digitales, las operaciones comerciales realizadas a través de sitios de Internet, en que los sujetos activos se valen de publicaciones digitales para ofertar productos, bienes y/o servicios a sabiendas de que no cumplirán sus obligaciones, y logran que los interesados

3 Palazzi, Pablo; *Los delitos informáticos en el Código Penal, Análisis de la Ley 26.388*, 1a ed, Buenos Aires, Abeledo Perrot. 2009, p.182-184

4 La estafa es una especie dentro del género defraudaciones, que se perpetra con ardid o abusando de la confianza en el sujeto pasivo

5 Donna, Edgardo; *Derecho Penal, Parte especial,* Tomo II B, Rubinzal-Culzoni editores, Buenos Aires, 2001, p. 273

inducidos en error anticipen pagos y/o transfieran sumas de dinero en su propio perjuicio o el de un tercero[6].

En este segmento de eventos, el dolo aparece en el inicio de las operaciones comerciales -lo que permite descartar incumplimientos de naturaleza civil- y se evidencia el uso de herramientas digitales como instrumentos de realización de los delitos, pero tales circunstancias no alcanzan para definirlos como ciberdelitos propiamente informáticos, dado que éstos surgieron con la tecnología, es decir con el nacimiento de la informática e Internet[7].

Como describe claramente Vaninetti[8], en las defraudaciones producidas en el medio virtual nos encontramos con dos tipos de "estafadores virtuales": a) Los que realizan fraudes mediante maniobras ardidosas tradicionales encuadrables dentro de la figura del art. 172 de nuestro Código Penal, que se perfilan como personas de conocimientos mínimos de informática puesto que necesitarán contar con conceptos básicos y elementales, y b) los otros casos de defraudación informática efectuados a través de la red y que encuadran en la figura del 173 inciso 16 que se logran a través de cualquier manipulación de un sistema de procesamiento de datos, y en donde ya se perfila la intervención de un individuo con conocimientos más profundos y específicos en cuestiones vinculadas con la informática. Dentro de este segmento los sujetos activos despliegan técnicas y procedimientos específicos de variada complejidad, como por ejemplo, el *phishing*.

3. La defraudación informática en particular.

El articulo 173 incorporó, tras la sanción de la ley 26.388[9], el inciso 16 por el cual se reprime al *"que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"*.

En el tratamiento dado al proyecto de ley, puede vislumbrarse que el legislador entendió

6 Ver sentencia del Juzgado en lo Correccional Nro. 1 del Departamento Judicial de Mar del Plata, en causa nro. 9.459/C (caratulados "Giménez Néstor Martín Olalla, María del Carmen; y otros s/ estafa (art. 172 del CP), de fecha 17 de Mayo de 2018. Disponible en https://bit.ly/37vxAba

7 Migliorisi, Diego; *Crímenes en la web. Los delitos del siglo XXI*. Editorial del Nuevo Extremo, 2014, Buenos Aires, pág. 37.

8 Vaninetti, Hugo A, *"Estafa en internet. Transferencia electronica de fondos. Operatoria de homebanking. La competencia en los delitos informaticos*, Sup Penal 2017 (febrero) LA LEY2017-A.312. AR/DOC/156/2017.

9 Argentina instrumentó cambios al Código Penal en el año 2008 mediante la sanción de la ley 26.388, incorporando y modificando figuras que permitiesen la tipificación de conductas en las que, especialmente, se veían componentes informáticos en su perpetración.

que dentro todas aquellas conductas disvaliosas en las que, utilizando un sistema informático como herramienta o tomando al sistema informático como objeto de la acción ilícita se produce un perjuicio patrimonial, la estafa informática ocupa, por su importancia, un lugar central. Con ese norte se destacó que prácticamente todas las legislaciones que se han ocupado del problema de la informática y su relación con el derecho penal han creado figuras especiales para reprimir estas conductas que, por otra parte, han sido objeto de diversas recomendaciones y convenciones emanadas de organismos internacionales[10].

Existió coincidencia en el debate parlamentario[11], respecto del "fraude informático", en cuanto a la conveniencia de incorporarlo dentro del capítulo sobre las defraudaciones. Se despejó así, definitivamente, las dudas suscitadas en los tribunales sobre dentro de qué tipos de delitos contra la propiedad debían subsumirse dichas conductas. La intención fue propiciar la redacción de un tipo penal que no generarse la clásica interpretación secuencial *ardid-error-perjuicio patrimonial*, ya que la imposibilidad de engañar a una máquina había generado lagunas de punibilidad en algunos casos. Por lo tanto se entendió que el nuevo articulo que sólo exige una manipulación informática sobre el sistema que provoque perjuicio, haría que el intérprete debiera apartarse de aquellos requisitos de la estafa clásica.

Incluso en ese sentido, se ha señalado que este artículo fue incorporado al Código Penal en miras de legislar sobre la modalidad del *phishing*[12] y aún sin ardid o engaño *"el legislador ha presupuesto, mediante una cláusula general, que el uso de una técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o trasmisión de datos, realizados para causar un perjuicio económico a un tercero, es una forma de estafa que se castiga conforme a la escala penal prevista para los diferentes tipos de fraude tipificados en el art. 173"*[13].

4. Conducta típica

Buompadre expresa que el tipo penal "*requiere el uso de un sistema informático como*

10 El instrumento por excelencia es la Convención de Budapest del año 2001, a la que Argentina adhirió y ratificó en el año 2017 mediante la sanción de la Ley 27.411.

11 Debate parlamentario Cámara de Senadores de la Nación. 18° reunión – 14° sesión ordinaria. 28/11/2007. Versión taquigráfica. También dossier publicado por Procuración General de la Nación. Ministerio Público Fiscal. Dpto. de Biblioteca y Dictámenes. Disponible en: http://www.rempm.org/archivos/Paginas/Grupos_de_trabajo/Crimen_Organizado/Delitos_Ciberneticos/ley-26388.pdf

12 Di Iorio, Ana H. (et. al).; *El Rastro Digital del Delito, aspectos técnicos, legales y estratégicos de la informática forense,* 1a. de. Mar del Plata, Universidad FASTA, 2017, Cap. 2. Pag. 133.

13 Buompadre Jorge, Manual de Derecho Penal, Parte especial. 3ra. reimpresion. Astrea, 2017, p 477

instrumento o medio a través del cual se produce el hecho lesivo del patrimonio ajeno. Se trata de un tipo de acción, por lo que la acción por omisión no parece posible; la referencia a cualquier técnica de manipulación informática impide toda consideración al respecto"[14].

Por su parte, Riquert señala que se ha tomado parte del proyecto de Ley de la Secretaría de Comunicaciones de la Nación (res. 476/01) en particular la fórmula "manipulación informática" sobre un sistema o la transmisión de datos (*data diddling o tampering*), pero no la referencia a que con ello se procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. Añade que dicha propuesta se veía con mayor rigor en el ejemplo provisto por el Código Penal español de 1995 que, en el punto 2 de su artículo 248, considera reos de estafa a los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero[15].

El mismo autor cita a Faraldo Canaba, quien en el medio español considera que por manipulación informática debe entenderse que la constituye toda introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos. Y aclara que este tipo de fraude informático no abarca los supuestos en que la utilización de las nuevas tecnologías de la información o las comunicaciones sea meramente circunstancial y, por eso, no pueda hablarse de "manipulación". Tampoco comprendería -según el autor- aquellos casos en que no medie relación de imputación objetiva entre las manipulaciones o artificios y la transferencia no consentida de activos patrimoniales, o los casos en que la manipulación sólo encubre otros delitos de desapoderamiento patrimoniales ya consumados (por ej., alterar el inventarío informatizado para ocultar la sustracción de mercaderías)[16].

Puede afirmarse entonces, que la acción típica consiste en defraudar a otro mediante cualquier técnica de "manipulación informática" que como señala Scheinsohn, puede producirse en cualquiera de las fases del procesamiento automatizado o manual, introduciendo, modificando, cambiando, reemplazando, suplantando, o alterando los datos existentes previamente, ya sea en el lugar de su almacenamiento o durante su transmisión

14 Buompadre. *Op. Cit.*

15 Riquert, Marcelo A.; *Código Penal de la Nación, Comentado y anotado*, Tomo II, Errius, Ciudad Autonoma de Buenos Aires, 2018, p. 1489/1490

16 Riquert, *Op.Cit,* p. 1490

total o parcial hacia o desde otros dispositivos, o hacia o desde otros individuos o personas físicas o jurídicas que se interrelacionen o que interactúen normalmente con ellos[17].

5. Modalidades de fraudes informáticos

Los autores mencionan varias formas de cometer fraudes informáticos, por ejemplo, la alteración de registros informáticos, la obtención de un servicio de telecomunicaciones sin haberlo abonado previamente, el fraude informático mediante interceptación de conexiones, el *phishing*, la estafa por *typosquatting*[18], la utilización de claves falsas, la sustracción de datos personales para utilizarlos en la web para efectuar compras on line, o las técnicas de "caballo de troya" o "técnicas del salami"[19].

Como hemos señalado antes, un sector de la doctrina considera que los casos donde el autor con cierta habilidad se hace dar la clave de un acceso a un sistema informático, ya sea telefónicamente o mediante *phishing*, quedan abarcados por la figura genérica del art. 172 del Código Penal.

Empero, respecto de esta tesis deben tenerse presente dos consideraciones: la primera es que como veremos el *phishing* es una técnica de ingeniera social, cuya modalidades y fines no se diferencia de otras, como el *vishing* por ejemplo; y la segunda, que la jurisprudencia es uniforme en considerarlos fraudes especiales del 173 inc, 16 del Código Penal. Así, se ha señalado: "*La figura penal en trato, al igual que en todas las formas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona. En el caso, la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso […]. [En el caso,] a través de una manipulación informática -acceso por cualquier medio y sin la debida autorización a una cuenta de correo electrónico del querellante- se provocó la transferencia de un activo con*

17 Scheinsohn,Marcelo; *La estafa informática* el Dial DC20F9, citado por Vaninetti, Hugo A, en *"Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informaticos*, Sup Penal 2017 (febrero) LA LEY2017-A.312. AR/DOC/156/2017.

18 Roibon, Maria Milagros; *La estafa informática en el Codigo Penal Argentino.* Disponible http://www.pensamientopenal.com.ar/doctrina/47322-estafa-informatica-codigo-penal-argentino

19 Figari Rubén, Reflexiones sobre la defraudación informática. Disponible en http://www.rubenfigari.com.ar/reflexiones-sobre-la-defraudacion-informatica-ley-26-388-2/

contenido apreciable económicamente (dominios de Internet) en perjuicio del patrimonio de [la víctima] y en beneficio del imputado. ..." (voto de los jueces Fernández, Fossati y Soto)[20].

6. Técnicas de ingeniería social

El principio que sustenta a la ingeniería social es que, en cualquier sistema, los usuarios son el **eslabón débil**. En este sentido, se ha señalado que no existe ningún sistema informático que no dependa, en algún punto, de un ser humano. Por lo tanto, la ingeniería social busca explotar la vulnerabilidad humana, que es independiente de la plataforma tecnológica[21].

Se define como *"el acto de manipular a una persona para que realice una acción que puede o no ser la mejor para lograr un 'determinado objetivo'. Esto puede incluir obtener información, obtener acceso o hacer que el objetivo realice una determinada acción"*[22].

Entre los vectores de ataque más frecuentes de la ingeniería social se encuentran tanto aquellos que explotan aspectos tecnológicos (como el *spam*, las ventanas emergentes de los navegadores, el uso de *software* malicioso, el *phishing*, el *pharming*, entre otros), así como también aquellos que se basan en el aspecto humano, explotando sus debilidades de comportamiento y aprovechándose de la voluntad de ayudar, del respeto a la autoridad, del temor a la pérdida de un servicio, entre otros, técnica que se conoce como *human hacking*[23].

En los fraudes informáticos, el uso de estas técnicas tiene lugar en el primer tramo del desarrollo de las maniobras delictivas: cuando los sujetos activos pretenden obtener los datos necesarios para acceder al sistema. El segundo segundo tramo implica que, una vez obtenida la información, se utilizan esos datos obtenidos capciosamente con el objeto de sustituir la identidad digital del usuario mediante la alteración de aquellos -por ejemplo claves bancarias- y la posterior transmisión de datos que se produce de manera ilícita y que implica necesariamente el despliegue de una acción tendiente a causar un perjuicio

---

20 Ministerio Público de la Defensa. Secretaría General de Capacitación y Jurisprudencia. Consulta destacada Jurisprudencia. Disponible en: https://jurisprudencia.mpd.gov.ar/Boletines/2016.08.%20Delitos%20informaticos.pdf

21 MOLIST, Mercè; *Ingeniería Social: Mentiras en la Red*; http://ww2.grn.es/merce/2002/is.html

22 Traducción propia de Hadnagy: *"Is the act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action".* Social Engineering: The Art of Human Hacking - Christopher Hadnagy (2010).

23 Instituto Nacional de Ciberseguridad de España (INCIBE). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/luchando-ingenieria-social-el-firewall-humano

patrimonial.

6.1. Phishing, vishing y smishing

El término *phishing* proviene de la palabra inglesa "*fishing*" (pesca), haciendo alusión a utilizar un cebo y esperar a que las víctimas "muerdan el anzuelo". La escritura *ph* es comúnmente utilizada por hackers para sustituir la *f*, como raíz de la antigua forma de *hacking* telefónico conocida como *phreaking*[24].

El ***phishing*** es una técnica que consiste en el envío por parte de un ciberdelincuente de un **correo electrónico** a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de obtener información privada, realizar un cargo económico o infectar el dispositivo, procurando suplantar la identidad del afectado. La forma más usual para lograrlo es adjuntar archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Cuando se utiliza la **llamada telefónica o de voz** para realizar la maniobra, se suele denominar ***vishing.*** El término es una combinación del inglés "voice" y *phishing*.

También puede producirse mediante el **envío de mensajes** ya sea por WhatsApp, mensajes de texto o servicio de mensajería de redes sociales, con el mismo objetivo. Este caso suele llamarse ***smishing,*** como contracción de los términos *SMS* y p*hishing.*

6.2. ¿Cómo funciona?

Los atacantes contactan con algún **motivo interesante**, como una oferta muy irresistible, o una posibilidad económica imprescindible (cobro de algún beneficio, ganarse un premio, entre otros). Es un motivo que apela a alguna emoción, para que la ocasión sea aprovechada. En general buscan captar la atención causando asombro, peligro o urgencia, que son emociones asociadas a la acción. Se utiliza el nombre de alguna institución, organismo, programa de TV muy conocido o de una empresa de renombre. Se aprovecha una situación específica o algo contextual: la pandemia, el cambio de gobierno, una decisión gubernamental, algún rumor urbano.

En ocasiones, los mensajes o artilugios discursivos empleados por los atacantes se

24 ***Phreaking*** o **pirateo telefónico** es un término acuñado en la subcultura informática para denominar la actividad de aquellos individuos que orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último; electrónica aplicada a sistemas telefónicos. El ***phreaker*** o **pirata telefónico** es una persona que con amplios conocimientos de telefonía podía lograr realizar llamadas gratuitamente.

vinculan con argumentos relacionados con la seguridad de la cuenta bancaria, o el adelanto de un trámite administrativo que justifique la necesidad urgente de entregar los datos personales.

Los atacantes intentarán forzar al usuario a que tome una decisión de forma inmediata, advirtiendo de peligros como consecuencias negativas si no lo hace. Aunque existen técnicas de ataques dirigidos, que comúnmente se conocen como *spear phishing*, en general los mensajes fraudulentos se generan a través de herramientas automáticas que integran funcionalidades de traducción y diccionarios de sinónimos por lo que suelen presentar faltas ortográficas y errores gramaticales

6.3. Ejemplos[25]

6.3.1. Entidades bancarias:


From: [redacted] [mailto:vbv@visa.com.ar]
Sent: Friday, March 01, 2013 9:40 AM
To: [redacted]
Subject: Ha ocurrido un error en su cuenta

[redacted] Online Banking

Estimado Cliente Sa[redacted]o:

Hemos recibido su información de acceso, la cual será sometida a Verificación por el Departamento de Seguridad En Línea del Banco.

Se le suguiere entrar al link que figura debajo para mayor seguridad del cliente. Para Normalizar su cuenta

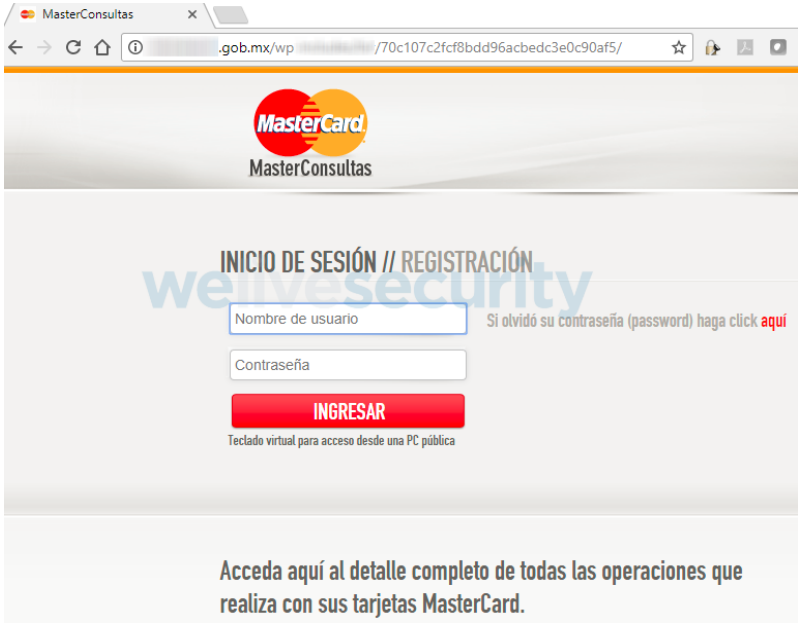
https://www.Personas.sa[redacted]io.com.ar/nb/ingresologin.jps

En este caso el **ardid de la maniobra** llega por correo electrónico, indicándose distintos mensajes capciosos como puede ser el cierre incorrecto de la sesión del usuario, la detección de una intrusión en sus sistemas informáticos, el bloqueo de la cuenta por motivos de seguridad, el cambio en la normativa del banco, las mejoras en las medidas de seguridad, entre otros. El **objetivo** en este caso es obtener números de tarjetas de crédito, tarjetas de coordenadas, PIN, token, usuario y contraseña.

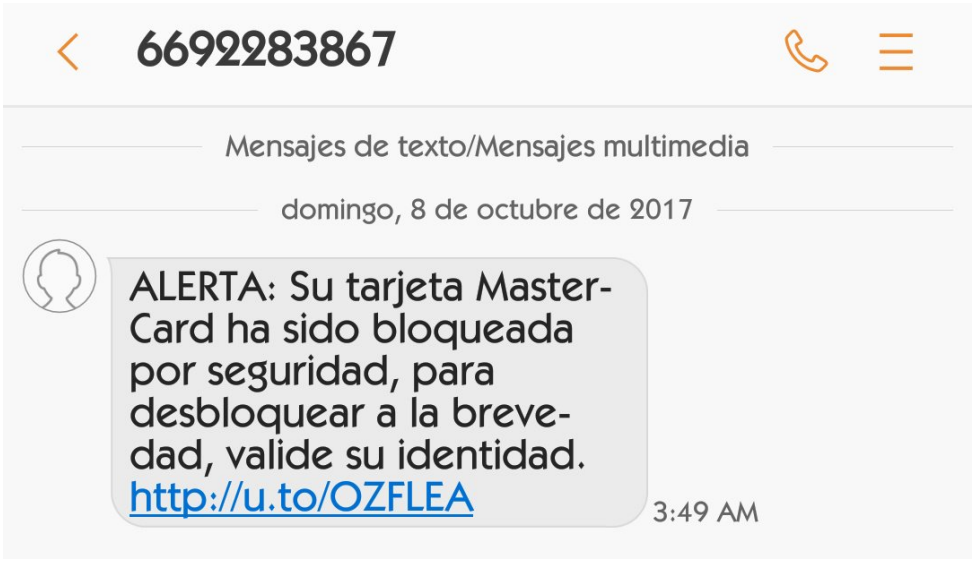
25 Imágenes tomadas del sitio *WeLiveSecurity* y *Oficina de Seguridad del Internauta* (OSI) de INCIBE, Instituto de Ciberseguridad de España: https://www.osi.es/es

6.3.2. Pasarelas de pago online (PayPal, Mastercard, Visa, etc.):

Nuevamente es a través de correo electrónico (*phishing*) procurando obtener claves de acceso o datos de tarjetas de crédito o débito, con el objetivo de utilizar dicha información en detrimento del usuario engañado.



A través de mensaje de texto (*smishing*):



En este caso, el **ardid de la maniobra** será el envío de un SMS donde se anuncia el

cambio en la normativa del servicio, el cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detección de una intrusión en sus sistemas informáticos, falta de pago de algún servicio, supuesto premio y número ganador, entre otros. En ocasiones el enlace puede permitir a los atacantes obtener información del dispositivo utilizado, o la descarga de aplicaciones conteniendo algún tipo de *malware*. El **objetivo,** al igual que en el caso del *phishing* anterior, principalmente obtener datos confidenciales para perjudicar patrimonialmente a la víctima.

6.3.3. Contacto telefónico:

En este caso, el **ardid de la maniobra** se despliega a través de una llamada telefónica en la que los sujetos activos simulan ser representantes de ANSES (o de cualquier otra entidad gubernamental o financiera) e informan a la victima que deberá dirigirse hasta un cajero automático para, manualmente, ingresar unos códigos y poder cobrar las sumas asignadas[26]. El **objetivo** al igual que en el caso del *phishing* anterior, consistirá en obtener los datos bancarios de la víctima o un tercero en su nombre, para luego acceder al *homebanking* y de esta forma, suplantar la identidad de la víctima con el fin de manipular el sistema y beneficiarse económicamente, perjudicándola patrimonialmente.

6.4. Adecuación típica de los casos de ingeniería social

Los ejemplos citados permiten visualizar, como ya mencionamos, que las técnicas de ingeniería social presentan características comunes, y que son empleadas en el primer tramo de las maniobras delictivas con la finalidad de obtener la información confidencial necesaria para acceder a los sistemas informáticos sin autorización de los legítimos usuarios[27].

En el segundo tramo del desarrollo de los delitos es que se presenta la manipulación informática propiamente dicha. Aquí, los sujetos activos usando la información obtenida, alteran los registros digitales y sustituyen la identidad digital del usuario para efectuar transferencias de dinero, obtener préstamos personales y/o ejecutar compras o ventas de

26 Véase por ejemplo: https://www.lavoz.com.ar/sucesos/millonario-cuento-de-ife-nacio-en-carcel

27 Este tramo de *iter criminis* considerado individualmente podría subsumir el hecho en la figura del art 153 bis del Código Penal que reprime *"...con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido..."*; sin embargo, en función del principio de especialidad y por configurarse desde el inicio un dolo tendiente a afectar el bien jurídico propiedad, la figura es desplazada por el art. 173 inc. 16 C.P.

divisas, o de productos o bienes o servicios, obteniendo beneficios patrimoniales en perjuicio de las víctimas o de terceros en su favor o en complicidad.

Nótese que el apoderamiento del dinero se produce sin conocimiento o voluntad del sujeto pasivo. Es decir, la víctima no ejecuta ningún acto dispositivo patrimonial y precisamente por ello, dentro de las exigencias del principio de legalidad, eventos de esta naturaleza no pueden ser considerados estafas, ya que uno de los requisitos legales para configurarlas es que como consecuencia del error, la victima del engaño sea quien realice un acto de disposición patrimonial.

Al respecto, como enseña Miro Linares, es el elemento de la transferencia autorizada o no lo que resultará determinante para la calificación jurídica: estafa en el primer caso o estafa informática en el segundo[28]. En definitiva, entonces, resulta determinante analizar a quién corresponde el dominio de la disposición patrimonial a los fines de la constitución como defraudación informática, entendiendo que no lo efectúa ni el sujeto pasivo ni tampoco al sistema informático: al primero por ausencia de voluntad y al segundo porque ejecuta las órdenes que le introduce el sujeto activo haciendo uso no autorizado de los datos de la víctima.

Y en ese sentido se ha considerado coautor del delito de fraude informático del art. 173 inc. 16 del Código Penal a quien mediante una técnica de manipulación informática conocida como *phishing* pudo conseguir de manera solapada los datos de usuario y contraseña del *homebanking* de la cuenta caja de ahorros del cliente de una entidad bancaria para posteriormente acceder al sistema informático y -alterando su normal funcionamiento- efectuar una transferencia de dinero con destino a una cuenta operada por un cómplice[29].

7. Conclusiones

Como hemos visto, para determinar el encuadre legal de las maniobras defraudatorias con el uso de ingeniería social dirigidas a obtener un beneficio económico, resulta clave establecer quién gestiona la información obtenida indebidamente para disponer del patrimonio, en tanto éste será el componente determinante para la adecuada calificación jurídica.

Como se evidencia de los casos repasados, el accionar de los sujetos activos apunta al

28 Riquert, obra citada, p. 1490

29 Fallo Domicent. IPP 08-00-25570-13/00, causa 6404 del Juzgado en lo Correccional N.º 5 del Dpto. Judicial Mar del Plata. Disponible para consulta en: https://bit.ly/38e0QUJ

factor humano como método de obtener información o claves que permitan acceder al sistema, siendo siempre éstos quienes disponen sobre los activos patrimoniales de las víctimas, las que bajo ninguna circunstancia expresan voluntad dispositiva. La ausencia de relación de causalidad entre el ardid, el error y la disposición patrimonial, pone de relieve la atipicidad de la conducta desde la figura de la estafa (art. 172, CP).

Por lo tanto, siendo que las disposiciones patrimoniales que ocasionan perjuicio obedecen a causas distintas a la voluntad del sujeto pasivo del delito, y que no son otras que al uso de técnicas de manipulación informática por parte de los sujetos activos que alteran la transmisión de datos, los casos de ingeniería social con estos aspectos fácticos, encuentran adecuación típica en el supuesto del articulo 173 inc. 16 del Código Penal.