RESPONSABILIDAD PENAL DEL RECEPTOR EN EL DELITO DE ESTAFA INFORMÁTICA. RESPUESTA JURÍDICO-PENAL DE LA JUSTICIA NACIONAL CRIMINAL Y CORRECCIONAL[1]

Agostina Magali Aguirre Álvarez[2]

1. INTRODUCCIÓN

A partir del año 2020 en función del inicio del aislamiento social preventivo y obligatorio ordenado por el gobierno argentino a raíz de la pandemia del COVID-19, muchas de las prácticas comerciales se volcaron a plataformas virtuales (Instagram, Marketplace, Whatsapp, OXL, Mercado Libre, etc.).

El avance de la tecnología de la información y comunicación (TIC), junto con el desarrollo de las operaciones comerciales en Internet, ha propiciado la creación de diversos mecanismos e instrumentos de pago, tal es el caso de Mercado Pago, billeteras virtuales o dinero electrónico.

El desarrollo de los instrumentos electrónicos de pago provocó el surgimiento de nuevas conductas delictivas, a la vez que contribuyó a la creación de ciertos patrones en la comisión de algunos delitos que dificultan su encuadramiento en los tipos penales tradicionales.

En el estudio de los supuestos delictivos cometidos a través de medios de pago, si bien ambas situaciones normalmente se traducen en la disposición indebida del dinero o del crédito asociado (en el caso de las tarjetas de crédito), con el correspondiente perjuicio económico para el titular legítimo, quien es el único autorizado para la utilización del instrumento de pago, es necesario diferenciar:

Por un lado, cuando el delito tiene por objeto el medio de pago en sí, como es el caso de la clonación de tarjetas o la falsificación, estas conductas se encuadran, en la mayoría de los casos, en el delito de estafa art. 172 y art 173 inc. 15 Código Penal de la Nación (CPN).

Sin embargo, cuando el medio de pago es el instrumento utilizado para la comisión de un delito que tiene lugar a través del uso ilícito del medio de pago –o de los datos asociados,

[1] Cítese como: Aguirre Álvarez, A.M. (2023). Responsabilidad penal del receptor en el delito de estafa informática. Respuesta jurídico-penal de la justicia nacional criminal y correccional. *Estudios sobre Jurisprudencia*, pp. 92-101.

[2] Abogada (Universidad Cuenca del Plata); Magister en Relaciones Internacionales (Universidad de Buenos Aires); Especialista en Garantías Constitucionales del Derecho Penal (Universidad Castilla La Mancha -España), Doctoranda en Derecho Penal y Ciencias Penales (Universidad del Salvador)

estos supuestos son abarcados por la figura de estafa informática, prevista en el art. 173 inc. 16 CPN.

La figura de la estafa informática fue incorporada al Código Penal argentino por la ley Nº 26.388 del 4 de junio del 2008 y es la que abordaremos en este trabajo.

El inciso 16 del artículo 173 del Código Penal de la Nación, la define como "aquella defraudación cometida mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos".

En otras palabras, este fraude se caracteriza por la obtención de un beneficio patrimonial a través de una manipulación informática.

Si tuviéramos que identificar un ejemplo práctico, imaginemos el caso de un autor desconocido "X", que ilegítimamente sustrae un celular a "Z". A las pocas horas, "Z" advierte que a través de su cuenta bancaria virtual (Mercado Pago, E-pagos, Ualá, Brubank, entre otros) se realizó una transferencia a "B", quien dispone de los fondos recibidos.

Partiendo de este caso simplificado, el artículo se propone visibilizar las complejidades y obstáculos que se presentan al analizar la relevancia penal –en términos de imputación objetiva– del sujeto titular de la cuenta bancaria receptora de la transferencia no autorizada a través del uso ilícito del medio de pago o, de los datos a él asociados, en el caso "B", al cual por razones metodológicas llamaremos en adelante "receptor".

2. DE LOS DELITOS INFORMÁTICOS A LA ESTAFA O FRAUDE INFORMÁTICO EN EL ORDENAMIENTO JURÍDICO ARGENTINO

Con carácter previo a examinar la problemática que subyace a los nuevos fenómenos delictivos, debemos detenernos en precisar que se entiende por delitos informáticos y específicamente como se recepta a la estafa informática en el ordenamiento jurídico argentino.

A tal fin, cabe aclarar que en la actualidad no existe una definición específica en cuanto al alcance del término "delitos informáticos".

A partir de la firma del Convenio de Budapest[3] podemos decir que existe una suerte de movimiento político criminal internacional orientado a punir los delitos que se realizan utilizando medios informáticos tanto como aquellos que se realizan teniendo como blanco sistemas y dispositivos informáticos.

[3] Consejo de Europa, 23.XI.2001 Convenio sobre la Ciberdelincuencia, Serie de Tratados Europeos No185, Budapest.

El significado más generalizado, entonces, es aquel que describe a este tipo de delitos como aquellas conductas indebidas e ilegales en las que interviene un dispositivo informático como medio para cometer un ilícito o como fin u objeto del delito mismo (Sain-Azzolin, 2018).

Nótese que sin perjuicio del concepto que se adopte, lo cierto es que se le asigna una importancia condicionante al lugar que ocupa la tecnología en el hecho, más que a la naturaleza delictiva del acto mismo. Y bajo esta lógica, este tipo de delitos poseen ciertas características propias desarrolladas por el medio en el que se cometen que condiciona su juzgamiento.

De esta manera, podemos identificar que, en el caso de los delitos informáticos, una gran mayoría de ellos son cometidos en forma anónima, sin rasgos personales del usuario a partir de la posibilidad de creación de identidades ficticias en la red (Sain, 2018). Asimismo, algunos de ellos son transnacionales, pudiéndose cometer desde una computadora y afectar a varios dispositivos en distintos puntos del planeta.

Ya adentrándonos en el tema que nos compete, en la actual sociedad de la información, son muchas las formas en las que se puede lograr acceder al patrimonio de terceros utilizando no solo las múltiples formas de relación comercial existentes en el ciberespacio sino aprovechándose de las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios.

Así, entre una variedad de fraudes que van transformándose constantemente, algunas de las más conocidas son aquellos realizados a través de la sustracción de los datos de las tarjetas de crédito, las estafas piramidales realizadas a través de Internet, las ventas online, así como los ataques de scam en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios o incluso operaciones de compra-venta lícitas.

De estas modalidades, con la sanción de la ley 26.388, conocida como la Ley de “Delitos informáticos”, se incorpora el inciso 16) al artículo 173 del Código Penal, el cual recepta la estafa informática y la define como “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”.

Dentro del catálogo de acciones abarcadas por el articulado precedente, el análisis se va a centrar en aquellas conductas defraudatorias que tienen lugar a través del uso ilícito del medio de pago –o de los datos asociados que se traduce en el correspondiente perjuicio económico para el titular legítimo, quien es el único autorizado para la utilización del instrumento de pago.

3. ÁMBITO DE COMPETENCIA: JUSTICIA NACIONAL CRIMINAL Y CORRECCIONAL

En este sentido no se puede soslayar que, a los fines del presente artículo, interesa la respuesta jurídico-penal de la Justicia Nacional Criminal y Correccional frente a esta modalidad delictiva.

Y el criterio de competencia no es otro que el de la propia naturaleza jurídica de la estafa tradicional o clásica.

En primer lugar, la figura en estudio se trata de un tipo especial de defraudación, cuya competencia genérica le corresponde a la justicia nacional, motivo por el que luce pertinente que su tipo penal especial, que regula el artículo 173, se investigue en la misma órbita.

Sumado a ello, se pondera que a través de estos últimos años se llevaron a cabo, por medio de convenios entre esta ciudad y el Estado Nacional (ley 26.702 -Convenio de Transferencia de competencias penales entre Nación y Ciudad Autónoma de Buenos Aires), distintas transferencias que especifican puntualmente que delitos pasaron a ser de competencia local, entre los que no se encuentra la figura investigada.

Y por último se adiciona lo expuesto por la Corte Suprema de Justicia de la Nación, a partir de su remisión a los fundamentos del señor Procurador en el caso "Zanni" (Fallos 333:589), en cuanto expuso que "no resulta admisible considerar inserta dentro de la competencia local a cada conducta ilícita que, con posterioridad a la ley 24.588 sea catalogada como delito en el sentido señalado por el juez correccional en su resolución sino que, contrariamente, los nuevos tipos penales que, eventualmente, se sancionen en el futuro, a menos que contengan disposiciones expresas, deben ser sometidos a un nuevo convenio de partes y posterior ratificación legislativa, para integrar la jurisdicción local" (dictamen del Procurador del 6 de agosto de 2009, S.C. Comp.83 L. XLV).

De tal modo, en sintonía con lo sostenido son las resoluciones dictadas por la justicia nacional criminal y correccional la base de este somero análisis introductorio a los problemas de imputación presentes en la estafa informática.

4. PROBLEMAS DE IMPUTACIÓN DEL SUJETO RECEPTOR

Para comprender como la situación particular de la estafa informática afecta el juzgamiento del sujeto receptor, resulta necesario traer a colación nuevamente el ejemplo disparador inicial: un autor desconocido "X", que ilegítimamente sustrae un celular a "Z". A las pocas horas, "Z" advierte que a través de su cuenta bancaria virtual se realizó una transferencia a "B", quien dispone de los fondos recibidos.

De este supuesto se desprenden dos cuestiones:

1. La identidad desconocida de aquel que sustrae o utiliza en forma no autorizada datos personales y cuentas bancarias de terceros.

2. La identidad conocida del titular de la cuenta bancaria receptora de la transferencia no autorizada, quien dispone de los fondos recibidos. En el caso, sería "B".

Por lo tanto, en este escenario, estaríamos en condiciones de afirmar que es "X" a quien le cabria –en principio– la autoría del delito de estafa.

Sin embargo, desde la *praxis* penal, simplemente se da por sobreentendido que estas conductas deben ser criminalizadas erigiendo al receptor como autor de la estafa, sin prácticamente ninguna fundamentación, pese a que, se trata de una conclusión que demanda una justificación precisa por los alcances de pena[4].

De esta manera, en la práctica, el receptor de los fondos deviene en el único imputado en el proceso penal aún sin conocerse con precisión su participación.

Ello en cuanto que, pese a ser muchos los intervinientes en este tipo de delitos, es al único que pueden identificar por el carácter de titular de la cuenta bancaria receptora.

Desde una perspectiva jurídica, entonces, el rol de "B" –titular de la cuenta bancaria receptora de los fondos enviados en forma no autorizada por "X"– plantea muchas dudas en tres cuestiones específicas: el tipo penal aplicable; la presencia de todos los elementos típicos exigidos dependiendo del delito del cual se trate, como también su forma de intervención.

Sin pretensión de exhaustividad, identifiquemos algunas situaciones a tener en cuenta al momento de analizar las conductas defraudatorias que tienen lugar a través del uso ilícito del medio de pago –o de los datos asociados que se traduce en el correspondiente perjuicio económico para el titular legítimo.

4.1. Del tipo penal

En primer lugar, recordemos que en este tipo de casuística se prescinde de la secuencia lógica reclamada por el delito de estafa genérica: ardid-engaño-disposición patrimonial perjudicial

[4] Respecto del tipo penal, el delito de encubrimiento conforme art. 277 CPN prevé "Será reprimido con prisión de **seis (6) meses a tres (3) años** el que, tras la comisión de un delito ejecutado por otro, en el que no hubiera participado (…)"; mientras que el delito de estafa conforme el art. 172 prevé "Será reprimido con prisión de **un mes a seis años**, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño…".

Respecto de la participación penal, el art. 45 CPN establece que "Los que tomasen parte en la ejecución del hecho o prestasen al autor o autores un auxilio o cooperación sin los cuales no habría podido cometerse, **tendrán la pena establecida para el delito**."; mientras que el art. 46 CPN "Los que cooperen de cualquier otro modo a la ejecución del hecho y los que presten una ayuda posterior cumpliendo promesas anteriores al mismo, serán **reprimidos con la pena correspondiente al delito, disminuida de un tercio a la mitad…**".

prevista en el art. 172 CPN (Aboso y Zapata, 2006; Mata y Martin, 2001; Faraldo Cabana, 2009). El nuevo precepto introducido por la ley 26388 permite, por lo tanto, circunscribir el escenario planteado al circunscriben el tipo penal del art. 173 inc. 16 de Código Penal.

En estos supuestos es dable observar que no hay un engaño hacia el titular de la cuenta bancaria como tampoco una disposición patrimonial por parte de esta última en función de aquel ardid.

Lo que aquí sucede es, por una parte, que la persona que sufre el error no es quien realiza el acto de disposición patrimonial como se exige en el modelo tradicional de estafa del Código Penal. Por el contrario, esta persona solamente entrega la clave de acceso al sistema de tratamiento de datos o aun cuando así no lo hiciera, es el propio sujeto activo quien una vez al interior de la plataforma bancaria realiza el acto de disposición patrimonial.

En efecto, el "engañado" lo que entrega es la clave y no el dinero que se encuentra depositado en la cuenta.

4.2. Del concepto de manipulación informática

Ahora bien, siendo la defraudación especial del art 173 inc. 16 CPN aquella cometida a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos, debemos definir qué se entiende por manipulación informática.

Siguiendo a Buompadre, podemos entender a la manipulación informática como toda modificación que implique una alteración o modificación del sistema informático, en cualquiera de las etapas del procesamiento, entrada (input), salida (output) o transmisión de datos (Buompadre, 2008)

En este sentido, el perjuicio patrimonial provocado por la realización automática de una transferencia no consentida de cualquier activo patrimonial debe traer su causa en cualquier técnica de manipulación informática, es decir en la modificación de resultado de un proceso automatizado de datos.

Y he aquí, el primer error al momento de analizar la conducta delictiva del Receptor.

Se pretende subsumir bajo el concepto de manipulación informática, toda conducta dirigida a la obtención y uso de datos para acceder al mecanismo electrónico de pago

En consecuencia, se soslaya que no toda obtención y uso de datos de acceso a plataformas de pago por la cual se genera la transferencia no consentida se trata efectivamente de una alteración o manipulación de sistema o de programa informático alguno.

Al continuar con esta lógica, solo se está realizando una generalización que resulta difícilmente aceptable desde el punto de vista del contenido del injusto típico. Además de incurrir en un error conceptual y terminológico.

4.3. De las diferentes técnicas de manipulación informática: phishing y pharming

En correlato con el punto anterior y entendiendo a la estafa informática como un entramado complejo, otro de los problemas que se presentan al momento del juzgamiento es la falta de un análisis más específico.

De las diversas técnicas de manipulación informática utilizadas para la obtención y uso de datos de acceso a plataformas de pago, por una cuestión metodológica, identificamos al phishing y pharming como aquellas que más incidencia presentan en el desarrollo de la conducta defraudatoria; pero no son las únicas.

En el caso del phishing, sucede que el sujeto lo que hace es ingresar a un sistema de tratamiento de información suplantando la identidad de otra persona que sí está autorizada para el ingreso.

En efecto, la entrada se realiza con una clave verdadera, facilitada por el titular de la misma pero su ingreso es indebido en el sentido que su uso no ha sido autorizado por su titular. Su empleo tampoco vulneró ni daño las barreras de seguridad previstas para el correcto funcionamiento e integridad del sistema. En otras palabras, no se ingresó alterando el software del portal web del instrumento de pago para así lograr una vía de ingreso distinta de la que se ha destinado por el programador.

Lo cierto es que la conducta de quien obtiene y/o hace un posterior uso de datos asociados a instrumentos de pago, se adecua a una suplantación de identidad titular del medio de pago.

El problema que trae aparejado esta acción es que precisamente la suplantación de identidad no está regulada en forma específica en nuestro ordenamiento jurídico y la fórmula penal del art. 173 inc. 15 y 16 CPN no contempla a la suplantación de identidad como medio comisivo.

La circunstancia señalada generaría un obstáculo al momento de encuadrar el accionar de quien emplea la técnica de phishing para obtener y hacer uso de datos de acceso a plataformas de pago en el tipo penal de estafa informática del art 173 inc. 16 CPN.

Caso contrario, sucede con la obtención y uso de datos a través de la técnica de pharming.

El pharming consiste precisamente en una manipulación sobre el sistema operativo informático tanto del titular de la clave bancaria, como también, de la plataforma de pago. De esta manera, se introduce un *malware* o un gusano en el servidor de Internet del usuario para

reconducirlo mediante la manipulación del Sistema de nombres de dominio (DNS) a una página web falsa[5].

En principio, al mediar una manipulación del Sistema de nombres de dominio (DNS) no supondría un problema ubicar el análisis del caso en la figura de la estafa informática.

En este sentido, se ha dicho que todo aquel que, a través de una manipulación informática provoque la transferencia de un activo patrimonial en beneficio propio o de un tercero y en perjuicio del titular del patrimonio lesionado, comete estafa prevista en el inc. 16 del art. 173 CPN (Buompadre, 2008)

4.4. De la autoría

Sin embargo, de insistir en el análisis de los casos en la figura del art. 173 inc. 16 CP, estaríamos luego frente a la dificultad de atribuir autoría al receptor.

Recordemos que receptor es el titular de la cuenta bancaria receptora de los fondos ilícitos.

La doctrina especializada define como mulas[6] a aquellos sujetos que facilitan al sujeto activo una cuenta bancaria de destino a los fines que se produzca la derivación del patrimonio del sujeto pasivo, el cual se obtuvo ilícitamente luego de la manipulación informática.

El punto problemático está en el hecho que, ya sea que hablemos de “money-mules”, “phishing-mules” o “pharming-mules”, y sin perjuicio de la problemática existente en relación al dolo[7], el receptor “mula” siempre realiza un acto que opera con posterioridad a la consumación de la defraudación patrimonial.

Bajo esta lógica, sostener –como sucede en la práctica penal– la autoría del receptor de fondos en función del art. 173 inc. 16 CPN, conlleva replantearse la figura penal elegida como marco de análisis de aquellas conductas que tienen lugar a través del uso ilícito del medio de pago o de sus datos asociados. Y en este caso, invocando la obra de William Shakespeare: estafa informática o delito de encubrimiento[8], esa es la cuestión.

[5] Ver Oxman, N., 2013. Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Revista de derecho (Valparaíso). Disponible en https://dx.doi.org/10.4067/S0718-68512013000200007 (último acceso 18.08.23)

[6] La conducta de estos sujetos ha sido abordada desde diferentes perspectivas jurídicas tales como delitos de narcotráfico y trata de personas (Sturla Lompré, 2021) y blanqueo de capitales (Llerena, 1998), como también por el ordenamiento jurídico español (Miró Llinares 2009; Fernández Teruelo, 2011)

[7] Ver análisis del tipo subjetivo del delito Ragués Vallès, 2007, La ignorancia deliberada en Derecho penal, 2007; Jakobs, 1995, Derecho Penal, Parte General, Fundamentos y Teorías de la imputación, Madrid.

[8] La doctrina argentina, en general, traza una línea divisoria entre la complicidad y las conductas posdelictuales de encubrimiento en función del momento en el que haya sido prestada la ayuda.

5. CONSIDERACIONES FINALES

A lo largo de este trabajo pretendimos visibilizar algunos de los diferentes obstáculos que plantea el análisis de la conducta del receptor en las defraudaciones que tienen lugar a través del uso ilícito del medio de pago o de los datos asociados, que se traduce en el correspondiente perjuicio económico para el titular legítimo.

En el particular, la intervención de estos sujetos en los delitos informáticos permanece exigua o ausente en la doctrina y jurisprudencia argentina.

La sofisticación de las técnicas que se utilizan para cometer delitos a través de Internet, la gran disponibilidad de herramientas modernas para hacerlo y la dificultad en términos de identificación del responsable de estas conductas –fundamentalmente a partir del uso de identidades ficticias y lugares de conexión públicos– hacen que los distintos sistemas judiciales queden desfasados ante esta realidad.

Estas características ya enunciadas, nos dan la pauta que la complejidad en su investigación provoca la preferencia de los tribunales en la aplicación de un criterio reduccionista puesto en un abordaje solo desde el punto de vista probatorio, evitando que la conducta del receptor sea analizada desde una perspectiva amplia, incorporando una mirada crítica e interdisciplinaria.

Entendemos que si bien contamos con una normativa adecuada –como lo es la llamada ley 26.388–, por sí sola la norma no es suficiente.

Por esta razón, espero que esta síntesis de las complejidades y obstáculos que conspiran contra un correcto juzgamiento de los delitos informáticos coadyuve a la comprensión y dimensionamiento de la estafa en entornos digitales en el ordenamiento jurídico argentino.

Bibliografía

Aboso, Gustavo E. y Zapata, María F., 2006. “Cibercriminalidad y derecho penal”. B d F.

Bacigalupo, E., 1996. Manual de Derecho Penal, 3a reimpresión, Hammurabi.

Bacigalupo, E. 1994. Lineamientos de la teoría del delito, 3a ed., Hammurabi.

Buompadre, J, 2008. Código Penal, Baigún-Zaffaroni, T° VII, Hammurabi.

Donna, E. A., 2014. Derecho penal. Parte General, Rubinzal-Culzoni.

Fernández Teruelo, J. G., 2019. Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red. Revista De Derecho Penal y Criminología Nº 19.

Jakobs, G., 1995, Derecho Penal, Parte General, Fundamentos y Teorías de la imputación, Marcial Pons.

Majid, Y, 2006. Cybercrime and society, Sage Publication.

Mata y Martín, R., 2001, Delincuencia informática y Derecho penal, Edi- sofer.

Mata y Martín, R., 2001. El robo de identidad: ¿una figura necesaria?, en V.V.A.A., 2010, Robo de identidad y protección de datos, Aranzadi.

Mir Puig, S. 2019, Derecho penal y teoría del delito, B. de F.

Romero, G., 2007, Delitos de estafa, Hammurabi, 2a. Ed.

Sain G. 2018 La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal en Cibercrimen y Delitos Informáticos, Suplemento Especial, Erreius.

Sain G., Azzolin H., 2018, Delitos informáticos. Investigación criminal, marco legal y peritaje, Editorial B de f.

Vallés, I, R, 2007. La ignorancia deliberada en Derecho penal. 4. Normativa nacional sobre ciberdelincuencia.