Escuela de Negocios

Universidad Siglo 21

ESPECIALIZACION EN CIBERCRIMEN

Trabajo Final de Graduación

Responsabilidad civil del imputado penal frente a delitos informáticos. Una aproximación hacia el análisis de la responsabilidad del imputado y de las entidades bancarias en las estafas informáticas.

HIDALGO MARIA LUZ

VECB000163

31104907

Tandil, febrero 2024

Resumen

El presente trabajo final versa sobre el análisis de la responsabilidad del imputado penal por los daños y perjuicios acaecidos delitos informáticos que involucren estafas bancarias y la posibilidad o no de acuerdo a la legislación de reclamar dichos daños tanto al imputado penal como a la entidad bancaria a través de la cual se perpetro el delito y asimismo el análisis de la posibilidad que tiene o no dicha institución de reclamar los daños y perjuicios al imputado penal ya sea en sede civil o sede penal constituyéndose como actor civil y sus implicancias procesales.

Se apunta a poder comparar la responsabilidad penal y civil del imputado o condenado, conjuntamente con la responsabilidad de la entidad bancaria atacada y si en caso de prosperar el reclamo debemos aguardar sentencia en sede penal para poder avanzar en nuestro reclamo civil por los daños y perjuicios generados y en tal caso quienes están legitimados activamente para dichos reclamos.

El auge de los delitos informáticos, especialmente las estafas bancarias, exige un análisis profundo de la responsabilidad civil y penal de los involucrados.

Este trabajo servirá para poder abordar posibilidades de reclamación tanto civil como penal para reestablecer el status quo previo al daño generado por una estafa informática, en este caso de contenido patrimonial como con las estafas bancarias perpetradas a través de medios informáticos.

Palabras clave: cibercrimen- reclamación civil – reclamación penal

Abstract

This final work deals with the analysis of the responsibility of the criminal defendant for the damages that occur in computer crimes that involve bank scams and the possibility or not, according to the legislation, of claiming said damages from both the criminal defendant and the banking entity. through which the crime was perpetrated and also the analysis of the possibility that said institution has or not of claiming damages from the criminal defendant either in civil court or criminal court, constituting itself as a civil actor and its procedural implications.

The aim is to be able to compare the criminal and civil liability of the accused or convicted, together with the liability of the attacked banking entity and if, if the claim is

successful, we must await a ruling in the criminal court to be able to advance our civil claim for damages. generated and in such case who is actively legitimized for said claims.

The rise of computer crimes, especially banking scams, requires an in-depth analysis of the civil and criminal liability of those involved.

This work will serve to address possibilities of both civil and criminal claims to reestablish the status quo prior to the damage generated by a computer scam, in this case of property content as with banking scams perpetrated through computer means.

Key words: cybercrime - civil claim - criminal claim

Índice

INTRODUCCIÓN

El presente trabajo final versa sobre el análisis de la responsabilidad del imputado penal por los daños y perjuicios acaecidos delitos informáticos que involucren estafas bancarias y la posibilidad o no de acuerdo a la legislación de reclamar dichos daños tanto al imputado penal como a la entidad bancaria a través de la cual se perpetro el delito y asimismo el análisis de la posibilidad que tiene o no dicha institución de reclamar los daños y perjuicios al imputado penal ya sea en sede civil o sede penal constituyéndose como actor civil y sus implicancias procesales.-

Dicho tema se encuentra enmarcado en el cibercrimen económico y para ello deberemos analizar en el desarrollo del presente el concepto de cibercrimen, los tipos de fraudes y ataques informáticos.

Se apunta a poder comparar la responsabilidad penal y civil del imputado o condenado, conjuntamente con la responsabilidad de la entidad bancaria atacada y si en caso de prosperar el reclamo debemos aguardar sentencia en sede penal para poder avanzar en nuestro reclamo civil por los daños y perjuicios generados y en tal caso quienes están legitimados activamente para dichos reclamos.

En la actualidad el avance tecnológico y el acercamiento a la información ha tenido un crecimiento exponencial y esto ha hecho que muchas tareas que antes precisaban de la presencialidad hoy en día se puedan llevar a cabo en la comodidad del hogar sin advertir los riesgos y lo observados que de todas maneras podemos estar.

La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), a cargo del fiscal general Horacio Azzolin, presentó su informe de gestión 2023 en el que analizó el aumento de los reportes asociados a la ciberdelincuencia registrados entre abril de 2022 y marzo de 2023. El documento destaca un aumento en las modalidades de fraude en línea, usurpación de identidad y secuestro de datos (ransomware) y un leve descenso en las maniobras asociadas a la compraventa de productos y estafas a través de servicios de billetera virtual.

La unidad especializada registró un incremento del 38,5% de los reportes recibidos, que pasaron de 25.588 a 35.447. Ello equivale 2.241 reportes mensuales.

Por otra parte, se incrementó en un 23% el número de investigaciones preliminares iniciadas por la UFECI: mientras que entre abril de 2021 y marzo de 2022 se registraron 287, durante el periodo abril 2002-marzo 2023 la cifra trepó a 353. La unidad especializada procesó

y analizó los reportes recibidos y logró identificar un gran número de conductas que derivaron en afectaciones masivas, con decenas -o incluso centenas- de víctimas, lo que implicó un abordaje estratégico.

El auge de los delitos informáticos, especialmente las estafas bancarias, exige un análisis profundo de la responsabilidad civil y penal de los involucrados. Este trabajo busca contribuir a la comprensión de este tema complejo, brindando herramientas para la defensa de los derechos de las víctimas. Mostrando la importancia practica que tiene la investigación de este tipo de delitos y de sus formas de responsabilidad. Este trabajo servirá para poder abordar posibilidades de reclamación tanto civil como penal para reestablecer el status quo previo al daño generado por una estafa informática, en este caso de contenido patrimonial como con las estafas bancarias perpetradas a través de medios informáticos. Entendiendo que hay algunas cuestiones no han sido tratadas por la doctrina como es el abordaje del actor civil en sede penal al momento de la reclamación en sede penal. Mucho se lee sobre la responsabilidad objetiva de las entidades bancarias en instancia civil, daños y perjuicios, consumidor, pero poco se habla de la posibilidad de que esas entidades puedan reclamar también al imputado a pesar de ser responsables por otra causa fuente.

Se debatirá y analizarán cuestiones relativas a las estafas informáticas teniendo en cuenta los siguientes interrogantes: ¿podremos reclamar civilmente al perpetrador del delito? ¿En qué casos podremos reclamar civilmente a la entidad bancaria? ¿podremos reclamar a ambos por los daños y perjuicios? ¿debemos aguardar condena en sede penal? ¿qué sucede en estos casos en los que no hay imputados claros o son delitos sin presos? ¿podemos utilizar el hecho de la víctima como eximente?

Debido a que este es un delito de amplio espectro y que se borran los limites internacionales debo acotar el alcance del trabajo por lo que apuntará a un análisis teórico y comparativo de responsabilidad civil y penal, sus eximentes y la posibilidad de reclamar por ambas vías, además de traer a la sede civil a la entidad bancaria a través de la cual se perpetro el delito.

Siguiendo a Saín podemos definir los delitos informáticos como "(…) cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución". (…) "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos" (Saín, 2018, pág. 9)

Teniendo en cuenta que los destinatarios de la carrera de especialización en la que se enmarca este Trabajo Final tiene muchos eslabones y uno de ellos pueden ser las entidades bancarias como sujetos pasivos de los reclamos y que como todos deben tener su debida defensa en juicio es que me interesa analizar la posible eximición de responsabilidad cuando se imputa y condena al autor material e intelectual del delito penal y la participación de los victima en las estafas informáticas a la luz del análisis de su responsabilidad para poder dilucidar en qué casos deben ser pasibles de eximición o no.-

El objetivo principal será identificar y evaluar el paradigma actual de responsabilidad de los imputados penales por delitos informáticos de estafa y su responsabilidad civil tanto ante el damnificado directo como ante la entidad bancaria afectada y la responsabilidad civil de esta última y su calidad de víctima.

Y dentro de los objetivos específicos tendremos: analizar la responsabilidad penal y civil de los imputados penales en las estafas bancarias; Clasificar los diferentes tipos de estafas informáticas que se evidencian en las principales entidades bancarias o de finanzas; Analizar los impactos negativos de las estafas informáticas en materia económica; Analizar las diferentes fuentes de responsabilidad civil; Investigar la responsabilidad civil de las entidades bancarias involucradas en delitos informáticos realizados por terceros; Analizar las vías de reclamación al imputado y a la entidad bancaria por las pérdidas sufridas por el delito de estafa bancaria; Analizar eximentes de responsabilidad; Identificar las responsabilidades en sentencias civiles y penales en casos de estafas informáticas; Identificar a las víctimas de los delitos informáticos

Con respecto al marco metodológico de la misma el presente trabajo tiene un enfoque o estrategia metodológica cualitativa. Al decir de Sampieri (Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. , 2014) este tipo de investigación utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. Por sus características (admite subjetividad, la posición del investigador es muchas veces explicita, la teoría es un marco de referencia, se generan hipótesis durante el estudio o al final de este) será la metodología viable para este trabajo.

Yuni y Urbano, (Yuni J.; Urbano. C., 2014) expresan que mediante esta estrategia metodológica se busca la captación del sentido de los fenómenos, se compara las propiedades de los fenómenos y se las analiza críticamente.

El tipo de investigación será descriptiva. Carlos Sabino en (Guevara Alban, G., Verdesoto Arguello, A., & Castro Molina, N, 2020) define a la investigación descriptiva en su obra El proceso de investigación como "el tipo de investigación que tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utiliza criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes". El investigador se limita a recoger la información que suministran los instrumentos de recolección de datos. Es necesario que el fenómeno estudiado sea organizado y analizado a la luz de un marco teórico apropiado, el cual servirá de sustento a la investigación.

Específicamente dentro del ámbito de la investigación jurídica será una investigación bibliográfica de tipo dogmática. La técnica de recolección y análisis de datos ser la documental, en tal sentido se recurrió a fuentes bibliográficas primarias, secundarias y terciarias, análisis de texto normativos, fallos, jurisprudencia, doctrina sobre el problema abordado.

Se analizó bibliografía especializada y de actualidad para luego analizar jurisprudencia de la materia que sirviera de base para el análisis.

El presente trabajo se centró en analizar las posibilidades que tiene la víctima de estafa por defraudación informática de reclamar por la vía civil y la vía penal el restablecimiento de lo sustraído, a través de la daños y perjuicios a las entidades bancarias y asimismo si podría a la vez de impulsar la sanción penal del imputado reclamar civilmente a este último.- Analizando si por ser diversas causas fuentes podría reclamar tanto al imputado como a la entidad bancaria la restitución de su dinero y/o daños y perjuicios, en el marco jurídico argentino. Asimismo, la importancia o no de la participación de la entidad bancaria en la causa penal como actor civil.

Se desarrollará el presente trabajo en distintos capítulos que nos llevarán de lo más general a lo particular, con una introducción, la delimitación y clasificación de los delitos informáticos, luego adentrándonos especificadamente a los delitos informáticos con contenido económico, para luego analizar a través de entrevistas, análisis de casos y jurisprudencia el estado actual de la cuestión y elaborar conclusiones.

El capítulo I aborda el concepto de cibercrimen, clasificando los delitos informáticos según su objetivo. Se discute la posibilidad de ejercer acciones civiles y penales independientemente en casos de daño material y moral, así como la responsabilidad de las entidades bancarias en casos de ciberdelitos. Se mencionan ejemplos de casos en los que las entidades bancarias no se constituyen como víctimas a pesar de sufrir pérdidas. Además, se

destaca la importancia de la intervención del actor civil en sede penal para garantizar la reparación del daño y promover la justicia.

El capítulo II aborda el tema de los delitos informáticos, centrándose en estafas y fraudes que afectan el patrimonio de las personas a través de la utilización de información sensible. Se mencionan casos específicos de fraudes con tarjetas, phishing, tabnabbing, man in the browser, spyware y skimming, así como ejemplos concretos de casos judiciales relacionados con estos delitos. También se discute el bien jurídico protegido en estos casos y se analiza la legislación al respecto. Además, se plantea la posibilidad de considerar a una entidad bancaria como víctima en un caso de delito cometido contra uno de sus clientes, y se analiza la relación entre las acciones penales y civiles, cuestionando la desigualdad de potestades entre los jueces penales y civiles. El capítulo también destaca la celeridad con la que las causas penales producen prueba y menciona la importancia de la intervención del actor civil en sede penal para garantizar la reparación del daño y promover la justicia.

El capítulo III se centra en la responsabilidad civil del imputado penal en casos de delitos informáticos, específicamente en el contexto de estafas bancarias. Se discute la posibilidad de ejercer acciones civiles y penales de manera independiente en casos de daño material y moral, así como la responsabilidad de las entidades bancarias en casos de ciberdelitos. Se analizan ejemplos de casos judiciales y jurisprudencia relevante, y se plantea la posibilidad de considerar a una entidad bancaria como víctima en un caso de delito cometido contra uno de sus clientes. Se analizan diversos mecanismos de reclamos y referencias legales y doctrinarias sobre el tema, así como la aplicación de la responsabilidad civil en situaciones de fraude financiero.

El capítulo IV aborda la responsabilidad civil del imputado penal en casos de delitos informáticos, centrándose en estafas bancarias. Se discute la posibilidad de reclamar daños y perjuicios tanto al imputado penal como a la entidad bancaria afectada, examinando las implicaciones legales y procesales de estos reclamos. Se destaca la importancia de la intervención del actor civil en sede penal para garantizar la reparación del daño y promover la justicia, y se mencionan los presupuestos para que ocurra la responsabilidad civil, incluyendo conducta ilícita, daño, relación de causalidad y factor de atribución. Además, se discute la responsabilidad objetiva, la responsabilidad por riesgo y la vulnerabilidad tecnológica en el caso de entidades bancarias.

CAPITULO I.- APROXIMACIONES AL CIBERCRIMEN

I.- Introducción:

El Capítulo I de este trabajo final de graduación se adentra en el concepto de cibercrimen, ofreciendo una clasificación de los delitos informáticos según su objetivo. Siendo este un capítulo introductorio donde veremos clasificaciones genéricas para avanzar a familiarizarnos con los términos. Este capítulo sienta las bases para comprender la complejidad y las implicaciones legales de los delitos informáticos, específicamente en el contexto de estafas bancarias.

I.II.-Aproximaciones conceptuales:

El National Institute of Standards and Technology [1] define cibercrimen como "delitos penales cometidos en Internet o ayudados por el uso de tecnología informática".

El cibercrimen suele perfeccionarse por medio de ciberataques que tienen por objeto afectar alguno de los pilares de la seguridad de la información.

Existen distintas formas de clasificar al cibercrimen. No obstante, podemos agruparlo según el objetivo que persigue, en tres grandes grupos, a saber:

- político;
- personal o social;
- económico

El cibercrimen económico es el más difundido, incrementándose los últimos años los delitos de pornografía infantil, grooming, ciberbullyng, sextorsión, entre otros.

I.III.-¿Qué es el cibercrimen? ¿Y los delitos informáticos?

El presente trabajo final de especialización parte de analizar los diferentes delitos informáticos, posteriormente se analiza la responsabilidad penal y civil de los imputados por estafas informáticas y la responsabilidad civil de las entidades bancarias para poder por último analizar la responsabilidad o hecho de la víctima y los posibles eximentes de los involucrados.

[1] https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary Recuperado el 20/12/2023

Con el objetivo último de concluir acerca de a quién y en qué casos podremos reclamar el daño patrimonial en este tipo de delitos.

Ahora bien, tal como sucede cuando se buscan definiciones, no es sencillo encontrar un solo concepto de delito informático.

¿Qué son los delitos informáticos? Siguiendo a (Saín, 2018) podemos decir que, si bien no existe una definición específica, desde la década del 70 esbozaron distintas acepciones en cuanto al alcance del término. Según el Manual de Recursos de Justicia Criminal del Departamento de Justicia de los Estados Unidos de 1979 se entienden por estas conductas a "cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución". Según una definición brindada por la Organización de Cooperación y Desarrollo Económico en 1983, el delito informático es "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos". (Saín, 2018, pág. 9)

La Organización para la Cooperación Económica y el Desarrollo define al "delito informático" como "Cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos. (Temperini, 2018, pág. 54)

En palabras del Lic. Cristian Borghello en (Temperini, 2018), "Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación".

En este sentido, consideraremos como incidente de seguridad a todos los hechos no deseados donde se comprometa de cualquier forma la seguridad de la información. Es decir, todos los delitos informáticos son, en el fondo, incidentes de seguridad de la información.

Por último, intentando analizar los conceptos en base a las diferencias o en términos de genero/especie, haré eco de las palabras del chileno Juan Pablo Cavada Herrera:

> *"…El término "cibercrimen" carecería de una definición universalmente homogénea y aceptada por los especialistas en el área, existiendo eso si acuerdo entre los investigadores en que sería una actividad ilegal realizada mediante un computador…"*

En base a eso hay homogeneidad de criterios, nadie creería que hablamos de cibercrimen utilizando un anotador y un birome. Aunque en algunas ocasiones podemos mencionar delitos que se perpetúan a través de ingeniería social a través de teléfonos, como el "cuento del tío"

que nos lleva a entregar información sensible o datos bancarios que finalmente se perpetúan a través de smartphones o computadoras.

Siguiendo con la definición de Cavada Herrera:

> *"...De las distintas definiciones doctrinales y de instrumentos internacionales, se desprenden diferentes conceptos, tales como delincuencia informática, abuso informático, criminalidad informática, criminalidad mediante computadoras, delitos informáticos, etc. Estos, se refieren, más que a una forma específica de delito, a una pluralidad de modalidades delictivas, vinculadas de algún modo con los computadores, designando una multiplicidad de conductas ilícitas y no una sola de carácter general, y parece hablarse de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.*
>
> *En síntesis, "delito cibernético" sería una acepción amplia, que comprende situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (por ejemplo, intromisión ilegal a bancos de datos), y aquellas en que dicho elemento es el medio para realizar un fin ilícito. De esta manera, el concepto de cibercrimen abarcaría, en sentido amplio, tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Y dentro de este término genérico, los delitos informáticos serían aquellas conductas delictuales en que se atacan bienes informáticos en sí mismos, no como medio, como por ejemplo, dañar el Software mediante la intromisión de un virus…."*
> (Cavada Herrera, 2020)

A través de este autor podemos ver como diferencia las acepciones para encontrar en ellas una diferencia por el objeto que ataca o el fin en si mismo.

I.IV.- Cibercrimen y cibercrimen económico

Cuando referimos al cibercrimen, Temperini (Temperini, 2018) nos indica que estamos hablando de una serie de delitos informáticos que ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas, donde los sujetos pasivos de los delitos son elementos fungibles y sin interés para el ciberdelincuente, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la

tecnología como eje. Si bien es posible encontrar ciberdelincuentes especializados que trabajan de forma independiente, es mucho más común encontrarlos organizados en bandas, con una clara distribución de tareas.

El concepto de cibercrimen económico se refiere a delitos penales cometidos en Internet, o ayudados por el uso de tecnología informática, que tienen por objeto generar algún tipo de beneficio económico para los atacantes.

En muchos casos, el cibercrimen económico se perfecciona por medio de ciberataques para obtener información que luego permite desplegar maniobras de fraude que generan réditos económicos a los criminales. Un ejemplo de esto puede ser el despliegue de un ciberataque para robar credenciales de acceso a una plataforma digital, de modo que luego los atacantes utilicen dichas credenciales para obtener ilegítimamente beneficios económicos.

Como se mencionará más adelante, el fin es lucrativo, lo que le interesa a los ciberdelincuentes es la información que obtiene por medio de medios electrónicos, que lo acercan en algunos casos a billeteras virtuales o al pedido de rescate a cambio de bitcoin para poder recuperar servicios.

I.V.- Conceptos generales de fraude e investigaciones

Las distintas tecnologías utilizadas por los medios de pago electrónicos y digitales actuales están expuestas a sufrir distintos tipos de ataques, los cuales dependerán, en parte, del ambiente en el que operen.

Por ejemplo, un cheque o una tarjeta son elementos físicos y, como tales, susceptibles a intentos de fraude físicos, como falsificación. Una plataforma digital estará expuesta a intentos de ataque lógicos o ciberataques.

Se habla de que los activos mas importantes en una organización son sus datos, la información que manejan y los eslabones mas débiles son los usuarios, las personas que manipulan esa información. Si esa organización o ese usuario no posee las medidas de seguridad apropiadas o no advierte que esta siendo victima de ingeniería social por ejemplo puede ser fácilmente vulnerado. La prevención y las políticas de mitigación de riesgos serán fundamentales.

I.VI.- Clasificación de tipos de delitos informáticos

Utilizaré la clasificación propuesta por Saín , donde indica que: "en la actualidad, los delitos informáticos pueden clasificarse en dos grandes grupos: aquellos que requieren de una sofisticación técnica para su comisión, generalmente basado en la elaboración de programas maliciosos desarrollados por hackers que buscan vulnerar los dispositivos o redes, generalmente con fines económicos y aquellos delitos que adquieren una nueva vida en la nube y son intermediados por servicios y aplicaciones web como las amenazas, los fraudes, el grooming . Muchos de ellos se cometen en lo que en informática se denomina "ingeniería social"(…) (Saín, 2018, pág. 11)

Luego hay otros tipos de delitos vinculados a la violación de la privacidad de los personas en tres niveles: "(…)Las intervenciones ilícitas de los gobiernos por sobre las comunicaciones privadas de los ciudadanos, como es el caso del espionaje ilegal de las agencias de inteligencia y seguridad de los Estados Unidos sobre ciudadanos extranjeros con programas de vigilancia en la lucha contra el terrorismo; la violación a la intimidad por parte de las empresas proveedoras de servicios de internet en términos comerciales sin el consentimiento del usuario para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados y el uso de la informática en el ámbito laboral, cuando en el marco de una organización empleadora se accede a comunicaciones privadas de un trabajador (mails, redes sociales, etc.) y lo despide del trabajo.(…) (Saín, 2018, pág. 11)

"…Otro autor que se anima a indicar características propias es el Dr. Julio Téllez Valdés, para quien los delitos informáticos presentan las siguientes características principales: 1. Son conductas criminales de cuello blanco (white collar crime), en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas. (…) 4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan. 5. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse. 6. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho. (…) 8. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico…" (Temperini, 2018, pág. 61)

I.VII.- Los delitos informáticos en argentina

En un principio, el Código Penal [2]de la República Argentina no tenía normas jurídicas que tipificaran los delitos que se originaban como consecuencia del uso de las nuevas tecnologías de la comunicación y la información. Paulatinamente comenzaron a aparecer figuras penales relacionadas con esta temática en diferentes leyes especiales.

Es una temática de mucha actualidad, por ejemplo, recientemente se aprobó en la Cámara de Senadores de Mendoza la figura del "agente encubierto digital". La propuesta servirá como una herramienta concreta, para que la justicia y la policía, logren luchar contra los delitos digitales, contra el abuso de menores y contra las estafas. De acuerdo a la iniciativa, en los casos de la investigación de delitos en que resulte necesaria la interacción en entornos o plataformas digitales, el Fiscal podrá requerir fundadamente ante el Juez Penal Colegiado, la actuación encubierta de un agente.

Volviendo al tema puntual del trabajo comenzaré con una definición de estafa en general y luego me enfocaré en la estafa informática.

El Capítulo IV del Título VI del Código Penal agrupa una variada gama de figuras delictivas bajo una denominación común "Estafas y otras defraudaciones". Al decir de (BUOMPADRE, 2009) las figuras que allí se encuentran conllevan un perjuicio patrimonial o lesión al patrimonio ajeno. Será el requisito para que nos encontremos frente a un delito estafa o defraudación y la estafa es el delito que consiste en un engaño por el cual una persona ve perjudicado su patrimonio en beneficio de otro. Obtenemos su definición del Artículo 172 del Código Penal de Argentina.

En el año 2008 se sancionó la ley 26388, que se la conoce como la ley de delitos informáticos. Esta norma tipifica como delitos e incorpora al CP varias conductas relacionadas con el uso de las nuevas tecnologías.

Las nuevas conductas tipificadas como figuras penales las presentamos de acuerdo a la clasificación realizada por la prestigiosa doctrina: a) Daño informático, agregándose en el artículo 183 del CP como segundo párrafo: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño"; b) Fraude informático, incorporando el inciso 16) al artículo 173 del CP en los siguientes términos: "El que defraudare a otro mediante cualquier técnica de

[2]Código Penal de la Nación Argentina (CPNA), (T.O. 1984 actualizado)

manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos". (Martínez, 2018, pág. 36).-

CAPITULO II. El delito de estafa o fraude informático

II.-Introducción

El Capítulo II se centra en los delitos informáticos relacionados con estafas y fraudes que afectan el patrimonio de las personas a través de la utilización de información sensible. Se analizan casos específicos de fraudes con tarjetas, phishing, tabnabbing, man in the browser, spyware y skimming, así como ejemplos concretos de casos judiciales relacionados con estos delitos. Además, se discute el bien jurídico protegido en estos casos y se analiza la legislación al respecto.

II.I.-Definiciones necesarias:

La estafa informática atenta contra el patrimonio de terceras personas, que "al igual que en todas las causas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona". (Martínez, 2018, pág. 38) El bien jurídico protegido es el patrimonio en general, y lo que se castiga son las conductas que afectan el patrimonio mediante el uso de sistemas informáticos por parte del causante.

Temperini en su trabajo plantea el problema del bien jurídico protegido indicando que como siempre en el derecho tenemos sectores planteando su postura. Por un lado tenemos el sector que plantea que son los mismos bienes tradiciones que tenemos que proteger y que sufren el delito por otros medios y por otro lado tenemos que el bien jurídico protegido es la información.

"…En palabras del Dr. Santiago Acurio Del Pino, "Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que a procesan o automatizan … Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere…" (Temperini, 2018, pág. 59)

Una de las características de los delitos informáticos: su carácter de **pluriofensivos**. Es decir, son delitos en los cuales es posible encontrar la afectación de más de un bien jurídico a la vez.

"…los aspectos que deben ser considerados de valor jurídico son la confidencialidad, la integridad y la disponibilidad de la información, es decir, los tres pilares de la seguridad de

la información desarrollados anteriormente. Desde esta óptica, será posible entender, por ejemplo, que en el caso de acceso indebido a un sistema informático, el bien jurídico afectado será la confidencialidad de la información. En el caso de daño informático (sabotaje para algunos autores), se afecta la integridad de la información. En el caso de la denegación de servicios, el bien jurídico afectado será la disponibilidad de la información…" (Temperini, 2018, pág. 60)

Pensemos en el caso del robo de los 165 millones de pesos en la comisaria de Santa Fe.[3] En este caso se sustrajo dinero destinado a pago de salarios, combustible y proveedores de una comisaría pero también se pudo haber tenido acceso a archivos confidenciales de detenidos, oficiales, causas policiales entre otros. Los delincuentes vulneraron las medidas de seguridad y, con ayuda del virus, "trabajaron" por meses para conseguir todos los datos necesarios para el robo. Los atacantes cibernéticos fueron pacientes y metódicos. Meses atrás enviaron una serie de correos electrónicos a la cuenta oficial de la Unidad Regional VI (Departamento Villa Constitución) de la policía provincial. Los remitentes decían pertenecer a la Empresa Provincial de la Energía, la Afip o Telecom. Alguno de los empleados del área administrativa contable de la fuerza hizo clic en una supuesta factura y así permitió el ingreso del troyano, un virus del tipo "bancario" que infectó el sistema y bajo su superficie comenzó a capturar información sensible relacionada con el manejo de dinero. Por semanas, con ayuda del malware, los ladrones fueron consiguiendo los elementos que necesitaban: credenciales de acceso a homebanking, token de seguridad, coordenadas. Finalmente, transfirieron la millonaria suma a medio centenar de cuentas no vinculadas entre sí.

Nuevamente la vulnerabilidad se vio afectada por la falta de prevención y educación de los agentes y de las personas que manipulan el activo mas importante hoy en día "la información".

La valoración económica sobre las pérdidas es totalmente subjetiva, ya que todo dependerá del tipo de información de que se trate.

Menciona Martínez (Martínez, 2018) en su artículo, en los casos de fraude informático es necesario descartar el error de la víctima llevada a cabo por el ardid o engaño del autor, pues este manipula una máquina con el objeto de obtener un beneficio económico en perjuicio

[3] https://www.ellitoral.com/sucesos/hackers-robo-policia-santa-fe-165-millones-villa-constitucion-ciberataque_0_72IbUoBuvb.html recuperado el 09/12/2023

patrimonial del afectado. Aseveración con la que no estoy de acuerdo en los casos en los que por ejemplo se perpetra el delito por ingeniería social o phishing.

Con la sanción de la ley 26388, conocida como la ley de "delitos informáticos", se incorpora el inciso 16) al artículo 173 del CP, el cual establece lo siguiente: "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". Con ello, ahora puede prescindirse de esta secuencia "ardid-error-perjuicio económico" y se amplían las posibilidades de encuadramientos de los distintos fraudes y estafas informáticas, incorporando cualquier forma de manipulación de un sistema informático con el objetivo de obtener un indebido beneficio económico en perjuicio de la víctima. (Martínez, 2018, pág. 36)

II.II.-Los delitos de fraudes financieros y económicos más comunes

Entre los delitos más comunes que sufren el sistema financiero y los titulares de cuentas bancarias podemos mencionar la alteración de registros informáticos con el propósito de ingresar a cuentas bancarias y desviar fondos a las cuentas de los delincuentes.

La suplantación de identidad por medio de cuentas de WhatsApp, de Instagram, en envío de mails con el objetivo de a través de phishing hacer caer en engaño a las víctimas, etc.

En el presente trabajo me ocupare de analizar las conductas sobre estafas y fraudes, es decir, aquellas donde el bien jurídico protegido es el patrimonio de las personas a través de la utilización de información sensible.-

II.III.- Man in the Browser (MITB)

Como se puede advertir la mayoría de los delitos pueden ser perpetrados producto de la desatención de las victimas. En este caso la persona debe instalar un programa, que contiene un malware que hará que se descargue un programa espia que logre capturar la información sensible que se utilizará luego para robar nuestros datos. Va desde activar nuestras webcam sin que lo notemos hasta copiar las combinaciones en el teclado al momento de ingresar a nuestros sitios bancarios.

"…Se trata de la instalación de un troyano (malware) en el navegador de la persona usuaria, que le permite al phisher capturar y modificar la información ingresada. La forma más usual consiste en la instalación de extensiones maliciosas del navegador creyendo que se trata

de aplicaciones legítimas. Una vez instalado el malware en el navegador, analiza el tráfico de datos a la espera de que se cargue una web considerada un objetivo…" (Ciberseguridad, 2021, pág. 4)

II.IV.-"Phishing" y "pharming"

Otro de los métodos de fraudes mas comunes es el conocido como phising y el pharming. Todos utilizamos correo electrónico en la actualidad y es común recibir en nuestras casillas infinidad de mails indicando que tenemos errores en nuestro home banking, que nos alertan por cambios de contraseñas, que es necesario verificar datos tal vez de entidades bancarias en las que ni siquiera tenemos cuentas.

A través de esos mails intentan engañar a usuarios que desprevenidos ingresan a esos mails y brindan sus datos personales reales en sitios falsos que luego bloquean sus cuentas, acceden a las mismas y dejan sin saldo o solicitan créditos a cargo de los damnificados.

> *(…) El phising, término anglosajón (escrito con "ph" en lugar de con "f") que alude a la pesca de datos bancarios a través de Internet, es una técnica fraudulenta que consiste esencialmente en la captación masiva ilícita de datos confidenciales de los usuarios de Internet.*
>
> *La actuación suele comenzar con el envío masivo de correos electrónicos a multitud de personas, que incluyen normalmente enlaces a páginas web, suplantando e imitando la identidad, imagen o apariencia de una entidad generalmente financiera o bancaria. En tales mensajes, utilizando diversos pretextos (seguridad informática u otros) solicitan el envío urgente de los datos de acceso bancarios, tales como la clave de usuario, contraseña, números de tarjeta de crédito, fechas de caducidad, etc. Una vez obtenidas las claves, se procede a realizar con ellas operaciones en la Red, normalmente transferencias de fondos sin el consentimiento de los legítimos titulares, normalmente hacia las cuentas de supuestos trabajadores captados mediante el envío de correos spam (las denominadas mulas).*
>
> *El pharming surge en abril de 2005 a causa de fallos de seguridad que se detectaron por aquellas fechas en los servidores de Microsoft204. La operativa se basa en la realización de manipulaciones técnicas de las direcciones DNS (Domain Name Server) que utiliza el usuario, de manera que cuando las escribe en el navegador le redirigen a páginas distintas de la deseada, si bien*

con un aspecto idéntico, creadas por los delincuentes. De esta manera obtienen sin consentimiento los datos bancarios o financieros que en manos de los delincuentes son empleados para operar en la red. (...) (Blanco Cordero I; Fabián Caparrós E.; Prado Saldarriaga V.; Santander Abril G. & Zaragoza Aguado J. , pág. 147)

Siguiendo el sitio "argentina.gob.ar" donde han elaborado un informe sobre guía y glosario del phishing, hare mención de algunas de las cuestiones que a mi entender son más importantes sobre este delito. (Jefatura de Gabinete de Ministros, Secretaria de Innovación Pública, 2022)

La expresión phishing es utilizada para definir a un tipo de fraude que tiene por objetivo engañar a la persona usuaria para que revele algún tipo de información, generalmente financiera o personal, con el objetivo de suplantar su identidad digital y obtener algún beneficio. Se trata del ciberataque más común y más sencillo, y quien lo perpetra suele ser denominado "phisher".

II.V.-Perjuicios del phishing para la persona usuaria

Como mencionaba al iniciar la definición hay infinidad de daños para la persona usuaria que es victima de estos delitos, y los mismos podemos definirlos de la siguiente manera:

"... van desde la pérdida de acceso a cuentas de correo electrónico, redes sociales, sitios de compraventa online hasta perjuicios y daños económicos derivados (...)El daño depende en gran medida de la información que el phisher haya sido capaz de robar y de lo que pueda hacer con ella. ..." (Ciberseguridad, 2021, pág. 1)

En la causa González Verónica Graciela c/ Banco de La Provincia de Buenos Aires y otro/a s/ nulidad de contrato, Tribunal: Cámara de Apelaciones en lo Civil y Comercial de Necochea, 9 de agosto de 2022, la damnificada sufrió un caso de phishing, se responsabilizó a la entidad bancaria por el deficiente control para impedir la efectivización de la maniobra de phishing de la que fue víctima un cliente. En sede civil la damnificada (actora) indica en su

demanda que el Banco debería haber iniciado causa penal contra el autor del hecho. La entidad bancaria al contestar la demanda negó su obligación de denunciar al autor del hecho.

II.VI.- Fraudes con tarjetas

La realidad económica actual hace que prácticamente no utilicemos efectivo, todas nuestras operaciones las realizamos con medios informáticos como billeteras virtuales o tarjetas de débito o crédito. Notesé que ahora la billeteras virtuales como Bullpay, Lemon (para utilización de criptos), Mercadopago, Personal Pay, etc nos brindan la posibilidad de acceder a una tarjeta de debito o crédito para utilizar en comercios.

La utilización de ese medio de pago hace que sea muy tentador para los delincuentes ya que de acceder a esa tarjeta se llega a los fondos con los que contamos en las billeteras o cuentas corrientes o caja de ahorro tradicionales, ni que decir de la posibilidad de utilizar el crédito disponibles de nuestras Visa o Mastercard, entre otros.

Por eso es importante definir este tipo de delitos y en palabras de Martínez leemos (…) Los fraudes con tarjetas abarcan a las de compra, crédito o débito cuando son falsificadas, adulteradas, hurtadas, robadas, perdidas u obtenidas ilegítimamente, tal como lo prescribe el inciso 15) del artículo 173 del CP. En tal sentido se ha dicho "que comete el delito de estafa en grado de tentativa el que utiliza la identidad y la tarjeta de crédito de otra persona para generar una compra a través de la red telemática" ("D. y G., P. J. s/procesamiento estafa" - CN Crim. y Corr. - Sala V - 30/6/2003, c. 21.774). Asimismo, "cuando el autor obtiene, de manera ilícita, una tarjeta de crédito de un tercero, al que le fue previamente sustraída, y la utiliza fraudulentamente mediante diversas extracciones dinerarias no autorizadas" (BGH 2 StR 461/05, sentencia del 13/1/2006). (…) (Martínez, 2018, pág. 40)

Otra maniobra fraudulenta muy común utilizada por estafadores con tarjetas bancarias es el uso de estas en cajeros automáticos, ya sea con tarjetas adulteradas o auténticas pero sin autorización del titular de la cuenta para obtener un beneficio económico.

II.VII.- Tabnabbing

Este tipo de delito es un poco mas elaborado ya que utiliza pestañas en segundo plano y también es necesaria la distracción de la victima para el ingreso de datos en sitios apócrifos.

"...Tabnabbing es un ingenioso tipo de phishing que apunta directamente a la vulnerabilidad de la persona usuaria. Este tipo de ataque nace del saber que muchas personas usuarias navegan por Internet usando muchas pestañas o ventanas a la vez. Entonces, mientras la víctima tiene en primer plano una pestaña determinada, el sitio malicioso reemplaza a una de las webs que estaban en segundo plano. Si la persona no se percata, ingresará sus datos en el sitio web del atacante, que suele indicar que se ha perdido la conexión o que la sesión ha caducado..." (Ciberseguridad, 2021, pág. 4)

II.VIII.- Cardado

Este sería el paso posterior al delito de skimming, a través del cual se va a verificar el saldo de las tarjetas clonadas para poder realizar compras. En general se hacen compras por pequeños montos para no alertar a los damnificados.

Se recomienda activar las alertas en los sitios como Visa home para registrar cada movimiento y poder denunciar al instante cualquier compra que no hayamos realizado.

(…) El cardado es un registro que utilizan los skimmers o clonadores vía internet o cajeros automáticos. Buscan verificar el saldo de las tarjetas electrónicas clonadas, mediante compras con montos pequeños para que el usuario o cliente no se alerte por la pérdida, retiro o transferencia.(…) (Martínez, 2018, pág. 43)

II.IX.- Skimming

Como mencionaba al principio al hablar de las tarjetas de crédito o débito, en este caso también son las destinatarias de los delincuentes.

(...) Son dispositivos colocados en los cajeros, monederos electrónicos, saldomáticos, pin pads, POS, skimmers, puertas de acceso, etc. Su objetivo es copiar en forma fraudulenta la banda magnética y el PIN de una tarjeta electrónica y luego la clonan o copian.(...) (Martínez, 2018, pág. 43)

Este término proviene del inglés, to skim (leer rápidamente u hojear), por lo que los delincuentes cuentan con diferentes dispositivos, conocidos como skimmers, para apropiarse de los datos sin que la víctima se dé cuenta. Generalmente, se lleva a cabo al realizar transacciones en un cajero automático o pagar en un terminal de punto de venta (TPV) manipulado previamente

> *(…)Cuando los delincuentes han obtenido los datos de las tarjetas bancarias, pueden realizar compras, contratar servicios o retirar dinero, entre otras transacciones, así como vender la información en el mercado negro para que sea un tercero quien materialice el fraude. También es posible que los estafadores se dediquen a hacer pequeñas compras para evitar ser detectados fácilmente. Este método se conoce como carding (…)*[4]

Este sistema podría ser también mas "rustico" y copiar o sacar una fotografía de los datos cuando vamos a abonar a algún comercio. Cada vez mas se recomienda no perder de vista la tarjeta al momento de pagar por ejemplo en un local comercial, restaurant, etc. O no dejar guardados los datos de pagos en las computadoras personales.

II.X.- Spyware

Podemos decir que es un software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario. Esto a menudo incluye la recopilación de datos confidenciales (como contraseñas, números PIN y números de tarjetas de crédito), la supervisión de las pulsaciones de teclas, el rastreo de los hábitos de navegación y la recopilación de direcciones de correo electrónico. Además de todo esto, estas actividades también afectan el rendimiento de la red, al ralentizar el sistema y afectar a todo el proceso empresarial.

Se instala sin nuestro consentimiento informado, ya sea una computadora tradicional, una aplicación en el navegador web o una aplicación móvil que se encuentra en tu dispositivo. (recuperado de https://latam.kaspersky.com/resource-center/threats/spyware el 27/12/23)

[4] Recuperado de https://www.santander.com/es/stories/skimming el 21/12/2023

II.XI.-Fraudes con tarjetas

La realidad económica actual hace que prácticamente no utilicemos efectivo, todas nuestras operaciones las realizamos con medios informáticos como billeteras virtuales o tarjetas de débito o crédito. Notesé que ahora la billeteras virtuales como Bullpay, Lemon (para utilización de criptos), Mercadopago, Personal Pay, etc nos brindan la posibilidad de acceder a una tarjeta de debito o crédito para utilizar en comercios.

La utilización de ese medio de pago hace que sea muy tentador para los delincuentes ya que de acceder a esa tarjeta se llega a los fondos con los que contamos en las billeteras o cuentas corrientes o caja de ahorro tradicionales, ni que decir de la posibilidad de utilizar el crédito disponibles de nuestras Visa o Mastercard, entre otros.

Por eso es importante definir este tipo de delitos y en palabras de Martínez leemos (…) Los fraudes con tarjetas abarcan a las de compra, crédito o débito cuando son falsificadas, adulteradas, hurtadas, robadas, perdidas u obtenidas ilegítimamente, tal como lo prescribe el inciso 15) del artículo 173 del CP. En tal sentido se ha dicho "que comete el delito de estafa en grado de tentativa el que utiliza la identidad y la tarjeta de crédito de otra persona para generar una compra a través de la red telemática" ("D. y G., P. J. s/procesamiento estafa" - CN Crim. y Corr. - Sala V - 30/6/2003, c. 21.774). Asimismo, "cuando el autor obtiene, de manera ilícita, una tarjeta de crédito de un tercero, al que le fue previamente sustraída, y la utiliza fraudulentamente mediante diversas extracciones dinerarias no autorizadas" (BGH 2 StR 461/05, sentencia del 13/1/2006). (…) (Martínez, 2018, pág. 40)

Otra maniobra fraudulenta muy común utilizada por estafadores con tarjetas bancarias es el uso de estas en cajeros automáticos, ya sea con tarjetas adulteradas o auténticas pero sin autorización del titular de la cuenta para obtener un beneficio económico.

II.XII.- Virus informáticos

Un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos.[5]

[5] Recuperado de https://ar.norton.com/blog/malware/what-is-a-computer-virus el 27/12/23

> *(...) Los virus informáticos son ataques destructivos, son realizados totalmente a través de las computadoras y en casos especiales con la complicidad de terceros, en forma física en determinadas eventualidades, de los cuales podemos citar los siguientes: 1. la propagación de virus informáticos destructivos; 2. envío masivo de correo no deseado o SPAM; 3. suplantación de los remitentes de mensajes con la técnica spoofing; 4. envío o ingreso subrepticio de archivos o keyloggers; 5. uso de Troyanos/Backdoors para el control remoto de los sistemas o la sustracción de información; 6. uso de archivos BOT del IRC y Rootkits para el control remoto de sistemas, sustracción de información y daños irreversibles; y 7.ataques a servidores con el objeto de sabotearlos.(...)* (Martínez, 2018, pág. 43)

Recientemente en la ciudad de Tandil, Pcia de Bs As, a propósito de un caso donde se vio afectada una gran suma de dinero por un virus informático (troyano), se logró recuperar el dinero de una gracias al rápido accionar de la Fiscalía de Cibercrimen UFI N° 22 de la ciudad de Azul.

II.XIII.- El caso

El día 21 de noviembre del 2023, se recibió una denuncia por parte de un empleado de una Empresa localizada en la ciudad de Tandil; dónde se pone en conocimiento de que había sido víctima de un troyano bancario, por el que fuera desapoderado de una suma millonaria; mediante transferencias del Home Banking del Banco Provincia de Buenos Aires que se destinaron a una cuenta elegida por el Cibercriminal que se hallaba en el Banco Provincia de Neuquén. El día 23 de Noviembre la Fiscalía pide el urgente secuestro del dinero existente en la cuenta de destino, el día 24 de noviembre el Juzgado de Garantías n° 1 de Tandil, otorgo la medida.

El día 1 de diciembre del corriente el Fiscal Moyano, ordenó la devolución del dinero retenido en favor de la víctima. Transferencia que se hizo efectiva el día 15/12/2023.-

El accionar hizo que se reintegren más de pesos $ 42.800.000 en favor de la víctima; pudiendo de esta forma dar una rápida respuesta.[6]

II.XIV.- Modalidades delictivas identificadas en informe de UFECI

La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), a cargo del fiscal general Horacio Azzolin, presentó su informe de gestión 2023. El documento detalla distintos modus operandi o situaciones delictivas reportadas durante abril de 2022 y marzo de 2023, entre las que se destacan los casos de fraude, que aumentaron un 33,2% respecto al periodo anterior. Mientras que entre abril de 2021 y marzo de 2022 se recibieron 19.854 reportes (3.156 por fraudes ligados a plataformas de banca electrónica y 8.740 a operatorias de compraventa), en el periodo actual se recibieron 26.454 reportes: 14.280 vinculados a compraventas y 3.418 relacionados con operatorias a través de la banca electrónica.

Desde la unidad especializada indicaron que en el periodo analizado se advirtió que, si bien la suba de este tipo de ilícitos se mantuvo en alza, fue menor (8,3%) en comparación con el aumento en el número de reportes totales y específicamente de casos de fraude.

Otra modalidad que registró un incremento fue el fraude cometido mediante usurpación de identidad. En el periodo comprendido entre los meses de mayo y julio de 2021 -el mismo periodo en el que se detectó una tendencia a la baja en los casos que involucraban plataformas de banca electrónica-, se pasó de 84 reportes a 280, un aumento del 233,3%. Esta tendencia se mantuvo en alza durante el periodo abril 2022-marzo 2023, que cerró con 491 reportes mensuales, habiendo alcanzado en noviembre de 2022 un pico de 522.

El informe indica que, en su mayoría los casos observados giraban en torno al uso de cuentas de plataformas de mensajería, en particular de la aplicación WhatsApp, bajo dos variantes. En una de las modalidades, los autores se hacían pasar por terceros y usaban cuentas asociadas a números telefónicos distintos a los de las personas cuya identidad suplantaban, aunque copiaban su imagen de perfil. En otros casos, la maniobra era más sofisticada, en tanto los autores lograban acceder en forma ilegítima a las cuentas cuya identidad suplantarían. En ambos casos, los perpetradores interactuaban con los contactos de la cuenta violentada y solicitaban transferencias a cuentas bancarias o billeteras virtuales con diferentes excusas.

---

[6] Recuperado de https://www.lavozdetandil.com.ar/2023/12/15/fiscalia-recupera-mas-de-42-millones-robados-en-ciberfraude-en-tandil- el 23 de diciembre de 2023

También hubo un incremento considerable -del 40,8%- en los reportes por accesos ilegítimos a cuentas. Mientras que en el periodo que va desde abril de 2021 hasta marzo de 2022 ese número ascendió a un total de 1.993 reportes, en los doce meses siguientes se relevaron 2.807 reportes, un aumento del 40,8%. Por ejemplo, las cuentas de Mercado Pago siguieron registrando accesos ilegítimos, mientras que en las cuentas de WhatsApp se incrementaron significativamente, pasando de 166 casos a 448, un 169,9% más.

La UFECI también indicó que no se advirtieron variaciones o incrementos relevantes en los reportes relacionados con posibles casos de ransomware, atravesados por la exigencia de criptoactivos, en tanto los pagos exigidos por los autores suelen solicitarse en esa especie. En tal sentido, los reportes se redujeron de 39 durante el periodo abril 2021-marzo 2022 a 20 durante el periodo siguiente.

En cuanto a las maniobras para obtener información confidencial mediante técnicas de ingeniería social, en las que los autores se hacen pasar por terceros (phishing), se indicó que "continúan ocupando un lugar preponderante dentro del ámbito de la cibercriminalidad". En tal sentido, entre abril de 2021 y marzo de 2022 se detectaron 2.129 reportes que aludían a sucesos que involucraron el despliegue de este tipo de técnicas -un 97,3% de aumento con respecto al periodo previo-, mientras que, entre abril de 2022 y marzo de 2023, los casos aumentaron a 2.975, lo que se traduce en un incremento marcadamente menor al anterior (39,7%), aunque denota una clara tendencia al alza.

El informe elaborado por la UFECI concluye que la tendencia al alza, en lo que respecta al número de conductas ligadas al cibercrimen, se consolida, pero aprecia que también lo hacen las técnicas y herramientas para su persecución, con foco en la capacitación de las y los agentes del servicio de justicia.[7]

[7] Recuperado de https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023/ el 21712/2023)

CAPITULO III.- RESPONSABILIDAD PENAL VS RESPONSABILIDAD CIVIL

III.- Introducción

El Capítulo III aborda la responsabilidad penal y civil del imputado penal en casos de delitos informáticos, específicamente en el contexto de estafas bancarias. Se examina la posibilidad de reclamar daños y perjuicios tanto al imputado penal como a la entidad bancaria afectada, y se analizan las implicaciones legales y procesales de estos reclamos. Además, se revisa la jurisprudencia relevante en el tema, con el objetivo de identificar y evaluar el paradigma actual de responsabilidad de los imputados penales por delitos informáticos de estafa y su responsabilidad civil.

III.I.- Análisis de las responsabilidades civiles y penales. Responsabilidad penal y sus presupuestos en Argentina

La responsabilidad penal es la obligación que tiene una persona de responder por un hecho punible. Dicha responsabilidad penal se encuentra regulada por el Código Penal. (Bertolino, 1998)

Los presupuestos de la responsabilidad penal son los siguientes:

- Tipicidad: El hecho debe ser previsto por la ley como delito.
- Antijuridicidad: El hecho debe ser contrario al ordenamiento jurídico.
- Culpabilidad: El autor del hecho debe ser imputable y debe haber obrado con dolo o culpa.
- Causalidad: El hecho debe ser la causa del resultado dañoso.

Tipicidad

La tipicidad es la adecuación del hecho a la descripción de un delito contenida en la ley. Para que un hecho sea típico, es necesario que se cumplan todos los elementos objetivos y subjetivos del tipo penal.

Antijuridicidad

La antijuridicidad es la oposición del hecho al ordenamiento jurídico. En el caso de la responsabilidad penal, el hecho debe ser contrario a la ley, es decir, no debe estar justificado por una causa legal o moral.

Culpabilidad

La culpabilidad es la capacidad de entender y querer la conducta antijurídica. Para que una persona sea culpable de un delito, es necesario que sea imputable y que haya obrado con dolo o culpa.

Causalidad

La causalidad es el vínculo que existe entre el hecho y el resultado dañoso. Para que una persona sea responsable penalmente, es necesario que su conducta sea la causa del resultado dañoso.

III.II.- Presupuestos de responsabilidad penal en Argentina

Principio de culpabilidad

En nuestro país, el principio de culpabilidad es la base de la responsabilidad penal. Esto significa que una persona no puede ser condenada por un delito si no es culpable.

Responsabilidad objetiva

En Argentina, existen algunos delitos en los que la responsabilidad es objetiva, es decir, que no se requiere probar la culpabilidad del autor. Los delitos de este tipo son, por ejemplo, los delitos culposos y los delitos contra la seguridad vial.

La responsabilidad penal es una institución jurídica fundamental que tiene como objetivo proteger el orden social. Los presupuestos de la responsabilidad penal son los elementos que deben cumplirse para que una persona sea responsable penalmente por un delito. (VAZQUEZ ROSSI, 2011)

III.III.- Responsabilidad civil

El autor de un delito como explique previamente puede y debe reparar penalmente si se lo encuentra responsable pero además puede reparar civilmente y estos son los presupuestos para que ello ocurra.

Siguiendo a (Bueres, Alberto y Zavala de González, Matilde, , 2016) podemos decir que para que la responsabilidad que genere el deber de indemnizar deben configurarse los presupuestos de procedencia exigidos por nuestro ordenamiento jurídico, es decir, una conducta ilícita o antijurídica, un daño, la relación de causalidad entre el daño y el hecho generador del mismo, y un factor de atribución de responsabilidad.

Es en este último punto, en el referido al factor de atribución me referiré a la entidad bancaria.

Siguiendo a (Mosset Iturraspe, 2017) diré que los presupuestos de la responsabilidad civil en Argentina son los siguientes:

Antijuridicidad: El daño debe ser contrario al ordenamiento jurídico. Esto significa que no debe estar justificado por una causa legal o moral; **daño**: El daño debe ser un perjuicio real y actual que cause una disminución patrimonial o extrapatrimonial; **factor de atribución**: El daño debe ser causado por el hecho de un agente, ya sea por su acción u omisión; **Relación de causalidad**: El daño debe ser consecuencia directa e inmediata del hecho del agente.

Estos presupuestos son comunes a la responsabilidad civil contractual y extracontractual. Sin embargo, existen algunas diferencias en su aplicación.

En la responsabilidad civil contractual, el factor de atribución es la culpa, es decir, la conducta negligente, imprudente o dolosa del deudor. En la responsabilidad civil extracontractual, el factor de atribución puede ser la culpa, la responsabilidad objetiva o la responsabilidad por riesgo.

La responsabilidad objetiva es aquella en la que el agente responde por el daño causado, sin que sea necesario probar su culpa. La responsabilidad por riesgo es aquella en la que el agente responde por el daño causado, aun cuando no haya sido negligente, imprudente o doloso.

En la práctica, la aplicación de los presupuestos de la responsabilidad civil suele ser compleja. En algunos casos, puede ser difícil determinar si el daño es antijurídico, si existe una relación de causalidad entre el hecho del agente y el daño, o si el daño es resarcible.

A continuación, se analizan con mayor detalle cada uno de los presupuestos de la responsabilidad civil.

Antijuridicidad

La antijuridicidad es un concepto jurídico que se refiere a la oposición del hecho al ordenamiento jurídico. En el caso de la responsabilidad civil, el daño debe ser contrario al ordenamiento jurídico, es decir, no debe estar justificado por una causa legal o moral.

Algunos ejemplos de daños antijurídicos son: La destrucción de un bien ajeno; la lesión a la integridad física o psíquica de una persona, la invasión de un derecho personal o patrimonial.

Daño

El daño es un perjuicio real y actual que cause una disminución patrimonial o extrapatrimonial. El daño patrimonial es aquel que afecta el patrimonio de la víctima, es decir, su capacidad de generar ingresos o sus bienes. El daño extrapatrimonial es aquel que afecta la persona de la víctima, es decir, su salud, su integridad física o psíquica, o sus derechos personalísimos.

Algunos ejemplos de daños patrimoniales son: El daño emergente, es decir, el gasto que debe realizar la víctima para reparar el daño causado. El lucro cesante, es decir, el beneficio que la víctima dejó de percibir como consecuencia del daño causado. Algunos ejemplos de daños extrapatrimoniales son:

El dolor y sufrimiento, la pérdida de la calidad de vida, la disminución de la capacidad laboral.

Factor de atribución

El factor de atribución es el elemento que vincula el daño con el hecho del agente. En la responsabilidad civil, el factor de atribución puede ser la culpa, la responsabilidad objetiva o la responsabilidad por riesgo.

Culpa

La culpa es la conducta negligente, imprudente o dolosa del agente. La culpa es el factor de atribución más común en la responsabilidad civil.

Responsabilidad objetiva

La responsabilidad objetiva es aquella en la que el agente responde por el daño causado, sin que sea necesario probar su culpa. La responsabilidad objetiva se aplica en los siguientes casos:

- Responsabilidad por el hecho de las cosas.
- Responsabilidad por el hecho de las personas.
- Responsabilidad por el hecho de los animales.
- Responsabilidad por riesgo

La responsabilidad por riesgo es aquella en la que el agente responde por el daño causado, aun cuando no haya sido negligente, imprudente o doloso. La responsabilidad por riesgo se aplica en los siguientes casos:

- Responsabilidad por el riesgo creado.
- Responsabilidad por el riesgo de la actividad.

Ejemplo de ello es el caso de la responsabilidad civil en los casos de accidentes de tránsito o en el caso de las entidades bancarias. Tal como indica el Dr. Ganino (ex Director Nacional de Defensa del Consumidor y Arbitraje del Consumo) en exposición del Colegio de Abogados de Azul del día 12/12/2023, las entidades responderán por los siguientes fundamentos:

- Dueño o guardián del sistema financiero informático.
- El propio Banco alienta a sus clientes a utilizar los sistemas telemáticos para realizar todo tipo de operaciones financieras (banca online).
- Contratos de adhesión.
- Generación de Confianza en sus clientes.
- In dubio pro consumidor.
- Perjuicio en los intereses económicos del consumidor.
- Deber de Protección y Seguridad de los Intereses Económicos de los usuarios financieros.
- Teoría del Riesgo creado y Riesgo Provecho.

- Vulnerabidad Estructural e Hipervulnerabilidad TECNOLOGICA (Res. 139/20 SCI)
- Responsabilidad OBJETIVA. (Art. 40 – 40 Bis Ley 24.240/ Art 1757 C.C.C.N)

Las circulares del BCRA que indican las medidas de seguridad que deben poseer estas entidades apuntan al tipo de responsabilidad objetivo.

Comunicaciones A 3682 y A 4272 : exige a los Bancos "...tener implementado mecanismos de seguridad informática que garanticen la genuinidad de las operaciones".

Estos fundamentos que menciona el Dr. Ganino en relación a la vulnerabilidad de la víctima, el perjuicio en los intereses económicos de la víctima, las directrices del BCRA, entre otras, fueron utilizados por ejemplo por el JUZGADO DE 1RA INSTANCIA EN LO CONTENCIOSO ADMINISTRATIVO, TRIBUTARIO Y DE REL. DE CONSUMO Nº 27 SECRETARIA UNICA dijo en el caso "KATZIN, VICTOR JORGE CONTRA BANCO PATAGONIA S.A. SOBRE CONTRATOS Y DAÑOS - RC - BANCOS, PRODUCTOS Y SERVICIOS FINANCIEROS", Exp. 115539/2022 que sentencio a la entidad bancaria y declaro la nulidad de las operaciones bancarias realizadas los días 02/01/22 y 03/01/22 y ordeno al Banco Patagonia SA, a que en el plazo de diez (10) días de que se practique la liquidación, restituya las sumas dinerarias respectivas en concepto de daño emergente, más intereses, asimismo condeno al Banco en la suma de pesos doscientos mil ($200.000) más intereses, en concepto de indemnización por daño moral y que además abone al actor la suma equivalente a tres unidades (3) Canasta Básica Total (CBT) Tipo Hogar 3 publicada por el INDEC (https://www.indec.gob.ar/indec/web/Nivel3-Tema-4-43), al valor vigente a la fecha del efectivo pago, en concepto de daño punitivo.

El caso que traigo a colación fue perpetrado mediante la maniobra de phising. El actor manifestó que el domingo 2 de enero de 2022 (día inhábil bancario y posterior a año nuevo), fue víctima de phishing. Unos ciberdelincuentes, mediante maniobras de manipulación psicológica, lograron obtener ciertos datos confidenciales para realizar numerosas operaciones fraudulentas en sus cuentas, todo ello sin control alguno u alerta del banco demandado.

Como manifiesta en la demanda todo comenzó cuando el actor intentó comunicarse con MERCADO LIBRE SRL (conocido como "Mercado Pago") vía TWITTER. Estaba realizando una operación

por dicha plataforma y el sistema se la rechazó, por la suma de $52.837, reteniendo su dinero. Como es sabido, dicha empresa no cuenta con un fluido canal de atención al cliente, por lo que el actor procedió a realizar el reclamo por dicha red social.

Necesitaba con urgencia que la empresa liberara sus fondos, para seguir operando.

En el transcurso de la media hora, el actor recibe el siguiente tweet de una cuenta con la absoluta apariencia de ser MERCADO PAGO El actor no dudó de la respuesta de la empresa (que se maneja exclusivamente por medios electrónicos) y ante la necesidad de seguir continuando con sus

operaciones por dicha plataforma, realizó la consulta al teléfono indicado, respondiendo a la palabra "consulta". A lo cual inmediatamente desde el número mencionado en el tweet una persona se comunica a la línea del actor en un tono muy amable, identificándose como representante de Mercado Pago, preguntando cual era la dificultad que tenía con dicha empresa, a los efectos de solucionar su inconveniente. Así las cosas, le solicitaron el número de transacción emitido por Mercado Pago, a lo que inmediatamente le brindaron el monto de la operación, su nombre y apellido, el apodo de su cuenta y la cuenta bancaria de Banco Patagonia S.A asociada a dicha aplicación. De esta forma, el actor sintió la absoluta certeza de estar hablando con representantes de Mercado Pago.

Seguidamente, le indicó que dicha plataforma se maneja a través de datos biométricos –lo cual es cierto, generando mayor confianza en el actor- por lo cual, para solucionar el inconveniente, maliciosamente le solicita una serie de datos para "liberar" los fondos.

Ante la necesidad imperiosa de contar con el dinero retenido por la aplicación, el Sr. Katzin confió en la aparente representante de Mercado Pago, pero lamentablemente, se trataba de un ciberdelincuente, que una vez que tomó el control de la cuenta de Banco Patagonia del actor, realizó una serie de numerosas operaciones fraudulentas, sin control u alerta alguna por parte del Banco. Cabe mencionar que el actor jamás brindó su usuario y clave de acceso a Home Banking. El ciberatacante se hizo de la clave "token" del actor, lo cual era desconocida su utilidad por parte del

Sr. Katzin. El banco jamás le informó debidamente para qué se utilizaba dicho códigoni que función tiene en el sistema, lo cual ya encontramos la primera falla del banco, en cuanto al déficit informativo hacia el accionante en cómo operar con los servicios electrónicos que la entidad ofrece. Hasta el día del hecho, el actor siempre realizó transferencias a través de CBU o ALIAS, debidamente agendado con tarjeta de coordenadas.

Continuando con el relato de los hechos, el actor detecta una situación irregular al momento en que no tiene acceso a la plataforma "Mobile" que brinda el Banco Patagonia para

ingresar desde el celular, y tampoco puede ingresar al home banking del Banco Patagonia desde su notebook. Inmediatamente, intenta comunicarse al canal de atención telefónico del banco a los efectos de bloquear su cuenta, sin éxito.

Claramente, el banco no tiene un canal de atención las 24 hs. ante delitos informáticos, ya que claramente, mucho de estos ilícitos se realizan en días u horarios no hábiles.

Aquí encontramos una nueva falla de la entidad demandada, que viola abiertamente con el trato digno y eficaz que los usuarios víctimas de estafas merecen, ante este tipo de situaciones límite.

Transcurrían las horas del domingo y el actor, desesperado y sin acceso a las plataformas digitales, se comunica al centro de atención al cliente del Banco Patagonia, para que el sistema automático (ya que no hay atención de personas de "carne y hueso") le informara los saldos de su cuenta en pesos y en dólares. Es allí cuando el actor termina de confirmar lo que sospechaba, es decir, que fue víctima de un engaño y consecuentemente, estafado. Así las cosas, el sistema automático del banco le informa los saldos de sus cuentas. En plena madrugada, los ciberdelincuentes procedieron a la sustracción de la totalidad de sus ahorros en dólares, en total MIL DOSCIENTOS (u$s 1.200), todas ellas en horario de la madrugada, donde curiosamente un cliente común no puede operar por ser un horario inhábil, pero el delincuente si lo pudo hacer, sin control por parte del banco.

El actor realizo denuncia policial ante por la División de Delitos Tecnológicos de la Policía Federal Argentina.

Asimismo, por tratarse de contratos bancarios, se aplican al presente caso las comunicaciones emitidas por el Banco Central de la República Argentina, que regulan la actividad bancaria.

Comunicación BCRA "A" 6017, 6878, 6664, 7072, 7175, entre otras.

Se tuvo en cuenta ademas la protección especial a determinados grupos con mayor vulnerabilidad en la relación de consumo, considerando consumidores hipervulnerables Res. 139/20 - SCI.

En cuanto a los alcances del deber de seguridad de la entidad bancaria, se sostuvo que "Los bancos cargan con el indelegable deber de seguridad a los fines de evitar este tipo de delitos —phishing—; no basta con ampararse en el cumplimiento de las normas bancarias predispuestas para librarse de su responsabilidad, sino que, por el contrario, deben ultimar los recursos y técnicas suficientes para mantener al cliente a salvo de las maniobras ciberdelictuales pergeñadas por terceros." (Cámara 2a de Apelaciones en lo Civil y Comercial

de La Plata, sala II, 05/05/2022, Suárez, Daniel Ricardo c. Banco de la Provincia de Buenos Aires s/ Nulidad de contrato" TR LALEY AR/JUR/63863/2022).

Con relación a la obligación de seguridad en cabeza de las entidades bancarias, nos encontramos frente a una obligación de resultado. Tanto el estatuto del consumidor, como la normativa del Banco Central de la República Argentina, pone en cabeza de las entidades bancarias desarrollar acciones tendientes a prevenir estafas virtuales.

De la causa se desprende las cargas impuestas a la entidad bancaria, la normativa del BCRA que debe primar en estas relaciones de consumo y que el actor realizo denuncia penal pero nada dice sobre la prosecución de esa denuncia por parte de la entidad bancaria que en definitiva abono por el delito de phishing realizado por el delincuente.

La importancia de este caso resalta en que a pesar de que el actor pudo haber brindado datos e incluso como indica el banco, no percatarse de que el tweet no estaba verificado, la responsabilidad recayó de todas maneras en la entidad bancaria producto de la vulnerabilidad del cliente y de la posición dominante del banco.

III.IV.- Relación de causalidad

La relación de causalidad es el vínculo que existe entre el hecho del agente y el daño causado. El daño debe ser consecuencia directa e inmediata del hecho del agente.

Para que exista una relación de causalidad, es necesario que el hecho del agente sea la causa necesaria y suficiente del daño.

Algunos ejemplos de relación de causalidad son: Un conductor que atropella a un peatón, Una empresa que fabrica un producto defectuoso que causa daños a un consumidor; un médico que comete un error en una operación que causa la muerte del paciente.

En los casos de las estafas bancarias resulta relevante la responsabilidad objetiva a los bancos, un ejemplo de ellos se encuentra en el fallo "Bieniauskas, Carlos c/Banco de la Ciudad de Buenos Aires s/ordinario" por los daños ocasionados a la víctima en un caso de phishing. El Tribunal actuante entendió "evidente que el sistema (software y hardware) que permite operar una red de cajeros automáticos puede ser calificado de cosa riesgosa. En rigor esta calificación puede ser asignada, en este punto al sistema informático que opera las

transacciones remotas, sea mediante el denominado home banking sea por el uso de cajeros automáticos". Y agrega: "Todos estos elementos, que revelan una reingeniería en la prestación de los servicios bancarios un incipiente pero constante cambio cultural hacia el uso de medios informáticos, son trascendentes para interpretar la conducta de las partes y la responsabilidad que sigue frente a un hecho irregular como el aquí analizado. Cabe reparar que el Banco al ofrecer a sus clientes un nuevo modo de relacionarse con él, debe procurar como mínimo, brindarle igual seguridad que si tal operatoria se realizara personalmente". Además sostiene "la posibilidad técnica de 'duplicar' las tarjetas no solo revela la falibilidad del sistema, y nuevamente su calidad de cosa riesgosa, sino también la irrelevancia de la conducta del actor en el punto". Asimismo afirma la atribución de responsabilidad objetiva expresando "sea que se invoque la ley de defensa del consumidor (art. 40, ley 24240), como de aplicarse el código civil (art. 1113), se arribará a igual resultado: asignar al Banco responsabilidad por lo ocurrido en tanto ambos supuestos prevén un sistema objetivo en esa materia". (Martínez, 2018, pág. 46)

III.V.- Sentencia penal y sentencia civil

Siguiendo a (Pizarro & Vallespinos, 2018) en nuestro país, la regla general es que la sentencia penal condenatoria produce efectos de cosa juzgada en el proceso civil respecto de la existencia del hecho principal que constituye el delito y de la culpa del condenado. Esto significa que la sentencia penal puede ser utilizada como prueba en el proceso civil para establecer la responsabilidad del demandado por los daños causados.

Sin embargo, existen algunos casos en los que la sentencia civil puede dictarse sin esperar la sentencia penal, como, por ejemplo:

- Cuando la acción civil se inicia antes de la acción penal. En este caso, el proceso civil se suspende hasta que se dicte sentencia penal.
- Cuando la acción penal se extingue por prescripción o por falta de mérito. En este caso, la acción civil puede continuar su curso.
- Cuando la sentencia penal es absolutoria. En este caso, la acción civil puede continuar su curso, pero el demandado puede oponer la excepción de cosa juzgada penal.

La regla general de esperar la sentencia penal antes de dictar sentencia civil y se basa en las siguientes razones:

Presunción de inocencia: La presunción de inocencia es un principio fundamental del derecho penal que establece que toda persona es inocente hasta que se demuestre lo contrario. Esta presunción se aplica también en el proceso civil, por lo que no se puede condenar a una persona por los daños causados hasta que se haya demostrado su responsabilidad penal.

Evitar sentencias contradictorias: La sentencia penal y la sentencia civil pueden versar sobre los mismos hechos. Si se dictan sentencias contradictorias, se puede generar una situación de inseguridad jurídica.

Eficiencia procesal: Esperar la sentencia penal puede ayudar a evitar que se dicten dos sentencias sobre los mismos hechos, lo que puede ahorrar tiempo y recursos.

III.VI.- Excepciones a la regla general

Las excepciones a la regla general de esperar la sentencia penal antes de dictar sentencia civil se basan en las siguientes razones:

Prevención de la prescripción: Cuando la acción civil se inicia antes de la acción penal, puede ser necesario dictar sentencia civil para evitar que la acción civil prescriba.

Necesidad de reparar el daño: Cuando el daño es irreparable, puede ser necesario dictar sentencia civil para reparar el daño a la víctima.

Presunción de culpabilidad: Cuando existen pruebas suficientes que demuestran la culpabilidad del demandado, puede ser posible dictar sentencia civil sin esperar la sentencia penal.

Y para el caso que aquí me interesa se destaca la excepción del Art. 1775 CCyC que en su incico c) indica: "…si la acción civil por reparación del daño está fundada en un factor objetivo de responsabilidad…".-

La decisión de esperar la sentencia penal antes de dictar sentencia civil es una decisión que debe tomarse caso por caso, teniendo en cuenta las circunstancias específicas del caso. Entiendo que, advirtiendo las particularidades de los casos de las estafas informáticas y su metodología, no sería razonable y volvería aún más injusto el padecer de la víctima que ve

como se deprecia su posible reparación y asimismo encuentra dificultades en encontrar un culpable penalmente responsable. (Pizarro & Vallespinos, 2018)

III.VII.- Importancia del actor civil en sede penal

El actor civil en sede penal es importante para garantizar la reparación del daño, ya que el actor civil es la persona que ha sufrido el daño como consecuencia del delito. Su intervención en el proceso penal es esencial para garantizar la reparación del daño, ya que el juez penal puede condenar al imputado a pagar una indemnización al actor civil, también puede contribuir a la investigación, aportando pruebas al proceso penal que ayuden a esclarecer los hechos y establecer la responsabilidad del imputado. Por último, su objetivo también será promover la justicia, al representar los intereses de la víctima y contribuye a que se haga justicia en el caso. (Pizarro & Vallespinos, 2018)

El CP en su artículo 65 nos indica:

"*ARTICULO 65.- Constitución.- Para ejercer en el proceso penal la acción civil emergente del delito, su titular deberá constituirse en actor civil.*

Las personas incapaces no podrán actuar si no son representadas, autorizadas o asistidas en las formas prescriptas para el ejercicio de las acciones civiles.

La constitución del actor civil procederá aun cuando no estuviere individualizado el imputado. Si en el proceso hubiere varios imputados y civilmente demandados, la acción podrá ser dirigida contra uno o más de ellos. Pero si lo fuera contra los segundos, deberá obligatoriamente ser dirigida, además, contra los primeros.

Cuando el actor no mencionare a ningún imputado, se entenderá que se dirige contra todos."

Tal como se observa no interesa aquí que el imputado este individualizado, por lo que todas las victimas podrían constituirse como actores civiles desde la primera presentación.

El actor civil en sede penal es una figura fundamental que contribuye a la reparación del daño, la investigación del delito y la promoción de la justicia. Su intervención es esencial para garantizar que las víctimas de delitos obtengan la reparación que merecen. En nuestro caso, es quien ha sufrido el daño y desea además de la condena del imputado la reparación que su accionar ha generado.

Como indica el art. 91 del Código Procesal Penal de la Nación “Facultades Art. 91. - El actor civil tendrá en el proceso la intervención necesaria para acreditar la existencia del hecho delictuoso y los daños y perjuicios que le haya causado, y reclamar las medidas cautelares y restituciones, reparaciones e indemnizaciones correspondientes.”

Debemos aquí dilucidar que será beneficioso para el damnificado:

Acción civil en sede penal: La víctima del delito puede iniciar una acción civil en sede penal, que se tramita en el mismo proceso que la acción penal. El juez penal puede condenar al imputado a pagar una indemnización a la víctima, que se ejecutará luego de que se dicte sentencia penal.

Advierta el lector que al indicar “puede” no quiere decir que sea de oficio ya que siempre será a pedido de parte interesada.

Acción civil autónoma: La víctima del delito puede iniciar una acción civil autónoma, que se tramita en un proceso civil independiente del proceso penal. En este caso, la víctima tendrá que demostrar que el delincuente es responsable de los daños causados, independientemente de que el delincuente sea condenado en el proceso penal.

Y asimismo si teniendo en cuenta las diferentes fuentes que originan la responsabilidad podremos reclamar por daños y perjuicios a la entidad bancaria a través de la cual se perpetro el delito en este caso por la responsabilidad objetiva que he descripto previamente.

¿Ahora bien…*podemos considerar victima a la entidad bancaria que ve como su patrimonio disminuye por afrontar una indemnización en sede civil por un delito cometido contra un cliente suyo*?

Entiendo que sí, ya que se puede considerar un damnificado indirecto al tener que absorber con su patrimonio el pago de los daños y perjuicios, la devolución del capital sustraído, el daño moral si se atribuye agregando además la publicidad que le genera y la pérdida de confianza que el público en general tendrá de conocerse la sentencia condenatoria.

También sería importante dilucidar si el patrimonio efectivamente se ve afectado o si en realidad es el asegurador del banco la principal víctima.

Las entidades bancarias no se presentan en las causas penales, no instan los tramites civiles contra los condenados ya sea por falta de confianza en la justicia o por no querer ventilar estos asuntos en sedes civiles que no cuentan con la confidencialidad que si cuentan las causas penales.

Esto bien lo podría suplir constituyéndose como actor civil en sede penal instando el trámite y solicitando al menos la restitución de lo sustraído, ya que en definitiva la entidad bancaria lo tenía bajo su custodia.

Volviendo a las sentencias penales y civiles, "…Para que opere la presentencialidad prevista en el artículo 1775 es preciso que concurran estos requisitos: pendencia de la acción penal antes de la promoción de la acción civil o durante la sustanciación de esta última, identidad de hecho y que no se configure ninguno de los supuestos de excepción que prevé dicha normativa.

No configurados los mismos, el juez civil puede resolver libremente, sin aguardar el decisorio penal.

En cambio, es intrascendente que en ambos juicios intervengan las mismas o distintas personas. Así, puede suceder que el damnificado civil "no haya querellado por el delito y que la acción penal haya sido incoada por el fiscal, como también puede ser que la acción civil se promueva por un damnificado indirecto que no está habilitado para intervenir en el juicio penal, o contra un responsable civilmente a quien no se puede acusar de nada ante el fuero criminal. En cualquiera de esos casos -u otros- en que hay *dualidad de procesos* originados en el *mismo hecho,* se impone la *postergación* de la sentencia civil hasta tanto se *dicte la sentencia penal y ésta quede ejecutoriada…"* (Pizarro & Vallespinos, 2018, pág. 613)

¿Habría identidad de hecho si reclamamos al autor penalmente responsable y a la entidad bancaria? *¿Y por otro lado la entidad bancaria al imputado/condenado penal?*

Esta parte entiende que no ya que si bien en la causa civil y en la causa penal serían las mismas partes la diferencia está en las fuentes y en el interés protegido.

El reclamo se fundaría en diferentes fuentes:

Reclamo a la entidad bancaria por su deber de seguridad, vulnerabilidad del sistema, en síntesis, todo lo mencionado por el Dr. Ganino.

Reclamo al imputado penal por daños y perjuicios ya sea en sede penal o de manera independiente en sede civil

Reclama la entidad bancaria al imputado penalmente responsable como víctima similar a una acción de repetición y en tal caso por los daños y perjuicios ocasionados por el accionar delictivo del ciberdelincuente y las consecuencias patrimoniales y publicitarias que la entidad bancaria debe responder.

Y aquí me surge otro personaje que será el asegurador de la entidad bancaria…¿o será que por su propio riesgo asumido no puede considerarse victima?

El daño de la entidad bancaria posiblemente no será reparado teniendo en cuenta las insalvables demoras de las sentencias, de los delitos sin preso y de la posible prescripción o absolución del imputado. Además de la necesidad de contar con seguridad jurídica y congruencia en las sentencias.

"…tendríamos que preguntarnos qué escándalo jurídico es más grave en la hora actual: si el que deviene de eventuales posibles sentencias contradictorias en determinados aspectos (existencia o inexistencia del hecho principal o existencia de la culpa del condenado en sede penal) o el que deriva inexorablemente de las tremendas demoras en la tramitación de las causas civiles cuando media presentencialidad penal. Demoras graves que no dejan de ser tales por el mero hecho de que no provoquen, en los hechos, una frustración efectiva del derecho a ser indemnizado. Esto último en la inmensa mayoría de los casos terminará siendo un cliché voluntarista e insincero, que sólo tendrá aplicación en los casos más groseros (Cromagnon, la tragedia de Once, Río Tercero), pero no en la inmensa mayoría de los casos, en donde los delitos culposos y los de naturaleza dolosa que no tienen preso, terminan en el insalvable destino de la prescripción…." (Pizarro & Vallespinos, 2018, pág. 670)

Pizarro y Vallespinos (2018) "…No hay justicia, porque la justicia que llega tarde únicamente tiene de tal su nombre…" (Pizarro & Vallespinos, 2018, pág. 587)

III.VIII.- Eximente - Hecho de la víctima o de un tercero por quién no debe responder.

"…*El cliente fue víctima de un delito, en el que la denunciada resulta ser un tercero." "Las acciones deben incoarse en el ámbito penal y exceden el marco de Defensa del Consumidor…"*

Esta serie de respuestas son las habituales en el marco de las relaciones consumeriles y reclamos ante la entidad bancaria.

Es por esto que debo analizar el eximente de responsabilidad que intentan las entidades bancarias para desligarse de responsabilidad.

En los casos especiales como por ejemplo accidentes de tránsito, donde también se habla de responsabilidad objetiva, la aseguradora puede aportar elementos para endilgar la responsabilidad en la víctima, ejemplo de ello:

"…*Los demandados no han logrado revertir la presunción de responsabilidad que pesaba en su contra, al no haber probado que se haya producido la ruptura del nexo causal, esto es, al no haber acreditado que el hecho ocurrió por el hecho de la víctima o de un tercero por quien no deba responder. Resulta de aplicación la teoría del riesgo, existiendo una presunción de causalidad entre el riesgo o vicio de la cosa y el daño acaecido, por lo tanto, la única forma de liberarse sería probando la interrupción de dicho nexo causal, por irrupción de otro hecho distinto, de la propia víctima o de un tercero extraño que desplace a la cosa y se erija a su vez en único, exclusivo y excluyente causante del perjuicio*…." (Partes: Toledo Alicia Norma y otro c/ Villalba Dante Ricardo y otros | daños y perjuicios; Tribunal: Cámara Nacional de Apelaciones en lo Civil; Sala/Juzgado: H; Fecha: 21-oct-2015; Cita: MJ-JU-M-95980-AR | MJJ95980)

Mas no puede hacer lo mismo la entidad bancaria atento a que sus obligaciones son distintas:

Fijémonos en el siguiente fallo de la Suprema Corte de la Provincia de Buenos Aires, "María Fabiana Gorrini C/ Banco de Galicia y Buenos Aires S.A" – 07/08/2020.- La Sra. María Fabiana Gorrini era titular de cuentas (caja de ahorro y cuenta corriente) en el Banco de Galicia y Buenos Aires S.A., el día 26 de noviembre de 2008, siendo las 20hs. aproximadamente, la actora usó un cajero automático en la Sucursal Banfield de la entidad financiera demandada, sita en la calle Hipólito Yrigoyen N* 7839, circunstancias éstas en las que fue víctima de un hecho delictivo. La entidad bancaria intenta desvirtuar su responsabilidad, por el obrar de un tercero (delincuente) por el que esa entidad bancaria no debía responder, pero el evento dañoso ingresa dentro de los riesgos inmanentes a la relación de consumo y es por ello que, más allá de quien protagonice el evento en sí, le cabe responsabilidad al banco como derivación del deber de seguridad que el ordenamiento tuitivo coloca en su cabeza.

Resulta un hecho notorio que muchas entidades bancarias pretenden desplazar la asunción de dicho riesgo al propio consumidor, ofreciéndoles la contratación de un servicio adicional de seguro por "robo en cajeros automáticos".

En este caso la entidad bancaria intentaba desligar su responsabilidad e incluso como menciona la Corte se le ofrece seguros con un costo adicional para el caso de delitos en sus cajeros automáticos.

Es interesante un trabajo en la Revista de Derecho Privado, n.º 35 de Colombia, cuando indica: "Es oportuno hacer otro tipo de reflexiones sobre lo que supone la existencia de culpa

de la víctima o del consumidor financiero, como causal de exoneración de la responsabilidad financiera; en efecto, vista la misma como elemento de disolución del nexo de causalidad, y teniendo en cuenta que la adecuación en la causa es requisito para su configuración, sería el caso de analizar si en los fallos de la Delegatura se exime o se mengua la responsabilidad de la entidad financiera en atención a un incumplimiento contractual del consumidor financiero, que además sea causa adecuada del daño. De otra parte, coincidiendo con algo sostenido con anterioridad, hay que señalar que el papel del consumidor financiero no puede ser de mero colaborador en la mitigación del riesgo, y por tanto no se le puede ver como quien tiene la carga de erradicación del mismo. Conclusión que se colige también de las consideraciones de la Delegatura, antes expuestas, en el sentido de que la garantía del riesgo le corresponde a la entidad financiera, por ser este un riesgo propio de su actividad (…)la consagración de la eximente de la culpa de la víctima tiene el propósito de salvar la inequidad que se daría si se obligara al virtualmente responsable a reparar efectos a los que no ha dado lugar, pero sería igualmente inequitativo eximirlo de reparar las consecuencias dañosas a las que sí dio lugar y en las que la culpa de la víctima no tiene ninguna injerencia causal.(…)" (Paz Sefair, 2018, pág. 274)

CAPITULO IV.- PROBLEMATICAS SOBRE LAS POSIBLES ACCIONES PROCESALES. DE LO SUSTANCIAL A LO PROCESAL. - VINCULACIÓN ENTRE LA ACCIÓN PENAL Y LA CIVIL CUANDO SE TRATA DE PUNIR Y RESARCIR DAÑOS.

IV .-Introducción

El Capítulo IV se adentra en la responsabilidad civil del imputado penal en casos de delitos informáticos, centrándose en estafas bancarias. Se examina la posibilidad de reclamar daños y perjuicios tanto al imputado penal como a la entidad bancaria afectada.

IV .I.- Problemáticas sobre las posibles acciones procesales

La temática es regulada por el Código Civil y Comercial en el Libro Tercero "Derechos Personales", en su Título V "Otras fuentes de las obligaciones" dentro del Capítulo 1 "Responsabilidad civil", en la Sección 11° "Acciones civil y penal".

El principio general está regulado en el art. 1774 CCyC, en el cual se expresa que "la acción civil y la acción penal resultantes del mismo hecho pueden ser ejercidas independientemente. En los casos en que el hecho dañoso configure al mismo tiempo un delito del derecho criminal, la acción civil puede interponerse ante los jueces penales, conforme a las disposiciones de los códigos procesales o las leyes especiales".

Es decir que un mismo hecho pueda dar origen a dos vías de reclamación. Ese será el punto de partida.

Asimismo, el mismo hecho puede dar lugar a que tanto el juez civil como el juez penal sea competente para juzgar los daños civiles.

Esto también me hace pensar en la desigualdad de potestades que tienen los jueces, ya que el juez penal podrá reparar civilmente en el caso de que se lo solicite, pero el juez civil no podría jamás inmiscuirse en el terreno del juez penal.

Bajo la órbita de que un solo juez con un mismo criterio analice todas las cuestiones se les acrecienten prerrogativas a los jueces penales que en tal caso no están en contacto directo con las nuevas directrices civilistas. Lo que en tal caso veo como positivo es la celeridad y la urgencia con la que las causas penales producen prueba.

"…El principio general está regulado en el art. 1774 CCyC, en el cual se expresa que "la acción civil y la acción penal resultantes del mismo hecho pueden ser ejercidas independientemente. En los casos en que el hecho dañoso configure al mismo tiempo un delito del derecho criminal, la acción civil puede interponerse ante los jueces penales, conforme a las disposiciones de los códigos procesales o las leyes especiales…" (Alferillo, 2015)

Advierta el lector que solo habla de daño material y moral, no hablamos aquí de lucro cesante o daño punitivo como si podemos hablar en las instancias civiles en causas donde el consumidor ve afectado sus intereses.

Menciona el autor previamente citado que la reparación civil en sede penal valdría para los casos de daño moral ya que no exige una prueba acabada dado que juegan a favor de su existencia presunciones hominis, razón por la cual siempre, ante la carencia o insuficiencia, de pruebas puede ser determinado prudencialmente por el juez.

En estos casos habría que analizar pormenorizadamente la posibilidad de reclamo de daño moral de las entidades bancarias, para ello hago eco de un fallo que niega dicha tal legitimación:

"…Procede rechazar el resarcimiento por daño moral pretendido por la sociedad actora. Ello por cuanto, cabe recordar que se ha entendido, en este sentido, que las personas jurídicas o de existencia ideal pueden ser sujetos pasivos de daños patrimoniales si soportan el ataque de sus bienes materiales, o sea, si sufren perjuicios patrimoniales directos, y podrían también reclamar reparación de perjuicios indirectos de esta índole, si fuesen vulnerados sus derechos extrapatrimoniales como el buen nombre, la probidad comercial y su buena reputación, si repercutiesen desfavorablemente en el patrimonio. Pero lo que en ningún caso podrían invocar es el resarcimiento del daño moral, porque no puede existir lesión a los sentimientos, ni alteración de un equilibrio emocional del que carecen, precisamente porque su existencia es puramente ideal para cumplir los fines de su creación y actuar en el derecho negocial dentro de la capacidad que tiene sus limitaciones en su objeto mismo. (cfr. Bustamante Alsina, "Las personas jurídicas no son sujetos de daño moral", ED 12/07/90; esta CNCom, esta Sala, 12/12/06, mi voto in re: "BVR SA C/ Banco Itaú Buen Ayre SA s/ ordinario")…."

Como indica Alferillo (Alferillo, 2015) es importante destacar qué sucede si hay sentencia penal de sobreseimiento o resuelve que el hecho no constituye delito penal o que no compromete la responsabilidad penal del agente, en tal caso se debe observar si en sus considerandos se examinó y determinó como acontecieron los hechos en cuyo caso por imperio

del art. 1777, bajo comentario, ello no producirá prejudicialidad sino que puede discutirse libremente el mismo hecho en cuanto generador de responsabilidad civil, ya que en ese caso se podrá discutir en sede civil el hecho como base fáctica para la reclamación.

IV .II.- Situación de las víctimas

En este último punto vislumbro a posibles víctimas. Ya mencioné que este es un delito pluriofensivo y que analizando las diferentes orbitas del delito encontramos a la víctima persona física que deposito su confianza en una entidad y que vio vulnerada esa confianza por el delito perpetrado por un ciberdelincuente. Por otro lado, tenemos al damnificado persona jurídica que será la entidad bancaria, bróker, billetera virtual que vio vulnerado su sistema de seguridad y que a pesar de que el ciberdelincuente ataco y llevo adelante la estafa es la entidad la que responde en el marco de la responsabilidad civil objetiva. La entidad aseguradora elegida por el banco para cubrir estos riesgos. Ya más en un sentido filosófico la Nación toda ve vulnerada su seguridad jurídica al ser constantemente atacada por ciberdelincuentes en pos de un redito económico.

Tal como indica Vazquez Rossi, se entiende por victima aquel sujeto que se postula o aparece como puntual y concretamente ofendido por hechos delictivos, es el sujeto pasivo de las acciones ilícitas, aquel que ha padecido de manera real, la ofensa criminal. (Vasquez Rossi, 2011).

La victima frente al proceso penal, puede asumir el rol de "particular damnificado" o "querellante", que es la victima legitimada dentro del proceso con patrocinio letrado y con las facultades y obligaciones que la legislación procedimental le otorga; o bien no asumir el mencionado rol y continuar como "victima propiamente dicha", conservando, aun así, una serie de derechos, prerrogativas y cargas procesales.

Quien se encuentra involuntariamente involucrado en el drama delictual, sufriendo una agresiva intromisión en la esfera de sus bienes jurídicos (libertad, integridad física, propiedad, etc.), percibe su necesidad de recibir una correspondiente reparación, que no se agota en el eventual resarcimiento económico o la punición del ofensor; sino que va más allá: su reconocimiento como sujeto del proceso penal, donde tiene mucho que decir y no puede ser un mero espectador. Ha surgido a fines del siglo XX el fenómeno que algunos autores denominan el "renacimiento de la víctima" (Bertolino, 1998), logrando reconocimiento y protección a su difícil situación.

Y exige su participación ya que esa persona es la que más cerca esta del delito y también porque la experiencia forense ha demostrado una serie interminable de casos de inactividad de los agentes fiscales en las investigaciones, lo cual desemboca indefectiblemente en la impunidad del crimen; esto hace indispensable, por caso, el control procesal de la víctima en lo que respecta a la etapa de instrucción, investigación, promoción y ejercicio de la acción penal, colección de prueba, etc.

Asimismo, podrá requerir el inmediato reintegro de las pertenencias sustraídas y hacer cesar

los efectos ulteriores del delito; bien puede tratarse de la devolución de cosas muebles sustraídas o el caso de inmuebles usurpados, etc; se da fundamentalmente en lo que respecta a delitos contra la propiedad y la idea es que el ilícito no rinda sus frutos

Advirtiendo que el particular damnificado podrá incorporarse al proceso penal, surgen dudas con respecto a las transacciones que podrán hacer entre actor y demandado. Por ejemplo, poder ser oídos tanto victima como imputado y eventualmente en el caso que este último expresa un sincero arrepentimiento, ofrezca resarcir el daño causado y efectivamente lo haga, se desinterese así a la víctima en la prosecución de la causa penal y no exista ninguna necesidad de política criminal, de imponer una pena; dadas todas estas circunstancias, finalmente se extinga el conflicto penal por caer en abstracto.

Pero si ocurriere esta situación, en los casos de estafas bancarias, *¿la entidad podría liberarse de responsabilidad por los daños y perjuicios generados al damnificado?*

Entiende esta parte que no, ya que una transacción entre delincuente y victima solo saldaría la deuda entre ellos mas no con la entidad bancaria, en la que ya no podría depositar su confianza, la que defraudo su seguridad y vulnero en algunos casos los ahorros de toda una vida.

¿Que causa fuente seria la que debe primar? La situación debería ser independiente, avanzar contra el delincuente por el recupero del dinero y los daños y perjuicios ocasionados, incluidos costas, gastos, honorarios y por otro lado la victima podría iniciar el reclamo ante la entidad bancaria. Lo único que debe primar es la justicia y el restablecimiento de los derechos conculcados.

¿Estaríamos hablando de enriquecimiento sin causa si reclamáramos por vía civil o penal a ambas partes? El art. 1794 del CCyC habla de este instituto "…Toda persona que sin

una causa lícita se enriquezca a expensas de otro, está obligada, en la medida de su beneficio, a resarcir el detrimento patrimonial del empobrecido.

Si el enriquecimiento consiste en la incorporación a su patrimonio de un bien determinado, debe restituirlo si subsiste en su poder al tiempo de la demanda….”

En este caso claramente no existiría tal cosa ya que estamos hablando de un ilícito, por lo que a todas luces la víctima, las victimas podrían reclamar el pleno resarcimiento por las vías que consideren y que son la que he mencionado previamente.

Lo que llama la atención es el desinterés por perseguir a los delincuentes por parte de las entidades financieras. La seguridad jurídica y su confianza está en juego y no pude hallar una sola causa donde la entidad vulnerada haya iniciado acciones civiles en contra del imputado.

Las entidades como brokers y billeteras virtuales responden puntualmente a los requerimientos de las oficinas de los fiscales, pero no se constituyen en actores civiles, no sienten conculcados sus derechos.

Habitualmente las personas nos acercamos a la entidad bancaria al advertir alguna situación extraña o al ver movimientos que no realizamos nosotros y allí advertimos que hemos sido estafados por lo cual se nos recomienda que iniciemos la denuncia penal para la correspondiente investigación.

Veamos un ejemplo: Juzgado Civil y Comercial 14, La Plata, FRIED CABRITA PATRICIA ANALIA C/ BANCO DE LA PROVINCIA DE BUENOS AIRES S/ NULIDAD DE CONTRATO, N° de Expediente: 60951/2022. En dicha causa, se responsabilizó al Banco a abonar la indemnización por deficiente seguridad y vulnerabilidades. La damnificada había hecho la denuncia correspondiente en la entidad bancaria y en la contestación de demanda se menciona simplemente que se contó con la denuncia penal pero nada hacen con ella.

Desde el sector de fraudes de las entidades bancarias se solicita como requisito la denuncia pero no se presentan posteriormente como víctimas directas o indirectas

En este punto nos acercamos a Comisaria o Fiscalía especializada y exponemos nuestros hechos, se nos pide documentación y luego se le pide documentación a la entidad bancaria.

Ahora bien, no es también la entidad bancaria victima de este delito? No debería también iniciar la investigación? Producto de que puede ser una persona ajena a la entidad o incluso un empleado o ex empleado infiel que ha vulnerado su sistema, además del hecho de

que al iniciar el reclamo por actor civil en sede penal o por daños y perjuicios de manera independiente es la entidad bancaria la que abona a la víctima un resarcimiento por un delito.

Hay ejemplos donde el imputado esta claramente identificado y aún así la entidad bancaria o broker no se constituye como particular damnificado.

Por ejemplo, en el departamento judicial de Azul, se encuentra en trámite la PP-01-01-003855-23-00, por ante TANDIL JUZ. G. Nº 1, investigación que lleva adelante la AZUL UFI N° 22, especializada en cibercrimen, el delito es Defraudación Informática - Art.173 Inc.16º. En dicha causa encontramos un imputado claramente identificado. El caso es de una defraudación informática, llevada a cabo a través de una billetera virtual donde se colocó el imputado como cotitular de la cuenta comitente, elimino a la titular primigenia y derivo todos los fondos de la cuenta a diversas cuentas, asimismo retiro por ventanilla una abultada suma de dinero. En este caso tenemos un imputado identificado, que retiro dinero por ventanilla, que se ve por las cámaras que no fue coaccionado a hacerlo, es decir, la entidad bancaria podría perfectamente iniciar acciones penales por la vulneración del sistema y por la pérdida de credibilidad que ahora ocasiona sobre su firma. Muy por el contrario, la entidad solo remite informes intentando posicionar a la damnificada como responsables del robo de credenciales.

Esto entendiendo siempre que los fundamentos de la reparación son diferentes en cada caso pero que el fin último es la seguridad y la credibilidad del sistema financiero y que se ve afectado cuando delincuentes intervienen en el cibercrimen económico.

Sería interesante pensar por qué no consideran que ellos también son víctimas si en definitiva son los que luego afrontar los gastos. O será por qué ellos tampoco son los que abonan esas siderales sumas de dinero que se aplican luego en las sentencias. ¿Al estar asegurados se desinteresan? Será materia de análisis para futuras investigaciones. Las empresas de seguros y reaseguros son en definitiva las más afectadas.

Son escasas las causas con condenados por la dificultad de identificar al autor penalmente responsable.

Encontramos por ejemplo: “Casación Penal confirmó condena por defraudación informática

La Sala III ratificó la pena de un año de prisión impuesta a un acusado, por haber manipulado los datos de acceso a la cuenta de un tercero a través de “home banking” y transferir dinero sin autorización de su titular, maniobra conocida como “phishing””

La Sala III de la Cámara Federal de Casación Penal, integrada por los doctores Eduardo R. Riggi, Liliana E. Catucci y Mariano H. Borinsky, confirmó la sentencia dictada por el Tribunal Oral en lo Criminal nº 18 de la Capital y condenó a la pena de un año de prisión a Pablo Alejandro Castelo, que el 18 de noviembre de 2011 mediante la manipulación indebida de datos informáticos obtuvo el usuario y las claves de acceso a la cuenta corriente de un tercero en el Banco Francés y a través del sistema "home banking" efectuó una transferencia de dinero sin autorización de su titular, maniobra conocida como "phishing". El monto de dinero defraudado fue transferido a una cuenta de caja de ahorro del Banco Francés y extraído mediante dos operaciones efectuadas desde cajeros automáticos de otras entidades bancarias. (51772/2011 - "Castelo, Pablo Alejandro s/recurso de casación" – CFCP – SALA III – 16/06/2015)

¿Por qué en estos casos se habla de estafas bancarias y el único que se presenta a perseguir al imputado es la victima o particular damnificado?

¿El banco solo requiere la denuncia para demostrar que la víctima no es responsable del hurto? ¿Qué beneficio tiene la entidad bancaria al solicitar una denuncia que luego el no impulsa?

Entiendo como dicen los autores Pizarro y Vallespinos (Pizarro & Vallespinos, 2018) que el proceso civil se caracteriza por su mayor, lentitud, la cual, en los días que corren, muchas veces deviene vejatoria para el justiciable. El proceso penal, en cambio, suele insumir menos tiempo, en razón del mayor dinamismo que presenta, fruto de las diferentes garantías constitucionales y principios procesales que lo orientan… El ejercicio de la acción civil en sede penal es, muchas veces, uno de los instrumentos de "persuasión" más eficaces que el damnificado cuenta y sin embargo las entidades bancarias dejan en mano de la justicia, pero no participan.

IV .III.- Derecho comparado

Un antecedente importante con respcto a la temática es el caso de Venezuela. Puntualmente resulta interesante un material de doctrina, el mismo se llama CUADERNOS DE DERECHO PROCESAL PENAL, Tribunal penal, indemnización civil y delitos informáticos, Nº 32, serie Doctrina (Lejed Cona, 2022) son una iniciativa de los miembros de la Sección de Derecho Procesal Penal del Instituto de Ciencias Penales de la Universidad Central de Venezuela, que tienen por cometido ofrecer a los estudiantes de Derecho Procesal

Penal, y al público en general que guarde interés por esta disciplina jurídica, exposiciones breves sobre tópicos o temas de esta área de la ciencia jurídica.

Como vengo manifestando quien ha delinquido es responsable tanto en el plano penal como en el plano civil, pero se trata de responsabilidades de distinta naturaleza y que están sujetas a normativas diferentes

Hasta ese punto estamos en igualdades conceptuales con nuestro país. Menciona que en sede penal existe la posibilidad de reclamo civil se presenta como una vía complementaria a la acción penal, permitiendo a la víctima buscar una compensación por los daños sufridos como consecuencia de un delito. Para poder iniciar este proceso, es necesario que exista una sentencia penal firme que establezca la responsabilidad del acusado. Distinto a lo que ocurre en nuestro país que para el caso de las estafas bancarias, por su factor de atribución, podemos iniciar el reclamo aun estando pendiente la causa penal.

El procedimiento penal venezolano especial regula detalladamente cómo se puede ejercer este reclamo civil, estableciendo que la demanda debe presentarse ante el mismo tribunal que dictó la sentencia condenatoria. Esta demanda debe cumplir con requisitos específicos y contener la solicitud de indemnización por los daños y perjuicios sufridos.

Esta posibilidad de reclamo civil en sede penal agiliza el proceso de obtención de compensación para la víctima, ya que se aprovecha la estructura y los recursos del proceso penal para resolver también la responsabilidad civil derivada del delito. De esta manera, se busca garantizar una reparación adecuada a la víctima y una justicia integral en casos de delitos que causan perjuicios económicos o morales.

La victima también puede dirigirse a los tribunales competentes en materia civil y ejercer la acción de manera autónoma. Entonces, la víctima cuenta con dos caminos procesales para un mismo objetivo y ante tal situación cabe destacar que los mismos se deben considerar como optativos, pues, la utilización simultánea de ambas vías procesales puede crear el problema de sentencias contradictorias lo que no beneficia a la víctima a los efectos de lograr la reparación o indemnización a la cual se considera con derecho.

Penalmente el procedimiento se denomina “Del procedimiento para la reparación del daño y la indemnización de perjuicios”. El trámite se detalla suscitamente:

1. Sentencia penal condenatoria firme. Para poder hacer uso de este procedimiento se requiere de la sentencia condenatoria firme

2. Ejercicio de la acción civil para la reparación de daños y la indemnización de perjuicios a través de demanda ante el tribunal que dictó la sentencia.

3. Admisión o inadmisión de la demanda dentro de los 3 días siguientes a su presentación.

4. Si se admite, el tribunal dictará la orden de la reparación de daños o la indemnización de perjuicios.

5. Intimación al demandado para cumplir con la reparación o indemnización u Objeción del demandado por escrito y con indicación de medio de prueba sobre la legitimación del demandante o por la clase y extensión de la reparación o monto de la indemnización al término de 10 días.

6. Citación de las partes a una Audiencia de conciliación si hay objeciones.

Si no asiste el requirente se archiva la demanda y si no va el requerido la orden de reparación o de indemnización se tendrá como sentencia firme y podrá proceder la ejecución forzosa

La admisión o inadmisión de la demanda es un aspecto de la lógica procesal civil. Si se admite, se dicta la orden de reparación de daños o de la indemnización de perjuicios y con ella se va a intimar al demandado.

Interesante es el hecho de que esta intimación logra convertir la reclamación en un titulo ejecutivo

Luego de la audiencia en el caso de que se realice se dicta sentencia admitiendo o rechazando la demanda. En el caso de que se le dé la razón al demandante se ordenará la indemnización o reparación adecuadas y las costas.

Advierta el lector la agilidad de este tipo de procedimiento especial para el caso de las estafas bancarias, donde probado el hecho dañoso es fácilmente demostrable cuál ha sido el perjuicio ocasionado para la víctima.

CONCLUSIONES

En el presente trabajo final de especialización comencé analizando el cibercrimen, comencé diciendo que el National Institute of Standards and Technology [8] definía cibercrimen como "delitos penales cometidos en Internet o ayudados por el uso de tecnología informática", se lo clasifico de diferentes formas en cuanto al objetivo de ataque; político, personal o económico. Luego de ello se definieron los delitos informáticos y Siguiendo a (Saín, 2018) se le definía como "cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución". Y para poder adentrarnos en los términos en base a los conceptos de genero/especie se utilizó la definición de Cavada Herrera:

Siguiendo con la definición de Cavada Herrera:

"…De las distintas definiciones doctrinales y de instrumentos internacionales, se desprenden diferentes conceptos, tales como delincuencia informática, abuso informático, criminalidad informática, criminalidad mediante computadoras, delitos informáticos, etc. Estos, se refieren, más que a una forma específica de delito, a una pluralidad de modalidades delictivas, vinculadas de algún modo con los computadores, designando una multiplicidad de conductas ilícitas y no una sola de carácter general, y parece hablarse de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

En síntesis, "delito cibernético" sería una acepción amplia, que comprende situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (por ejemplo, intromisión ilegal a bancos de datos), y aquellas en que dicho elemento es el medio para realizar un fin ilícito. De esta manera, el concepto de cibercrimen abarcaría, en sentido amplio, tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Y dentro de este término genérico, los delitos informáticos serían aquellas conductas delictuales en que se atacan bienes informáticos en sí mismos, no como medio, como por ejemplo, dañar el Software mediante la intromisión de un virus…." (Cavada Herrera, 2020)

Luego nos adentramos en el cibercrimen económico y siguiendo a (Temperini, 2018) , indica que en este tipo de delitos los sujetos pasivos de los delitos son elementos fungibles y

[8] https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary Recuperado el 20/12/2023

sin interés para el ciberdelincuente, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje.

Atento a que esta investigación tiene un particular interés en el eje económico de estos delitos, nos referimos al concepto de cibercrimen económico, que se refiere a delitos penales cometidos en Internet, o ayudados por el uso de tecnología informática, que tienen por objeto generar algún tipo de beneficio económico para los atacantes.

Posteriormente se analizaron los distintos tipos de delitos informáticos relacionados con aspectos económicos como, por ejemplo: fraudes con tarjetas de crédito, phishing, tabnabbing; Man in the browser; spyware; entre otros. A los efectos de poder dilucidar a través de que mecanismos los delincuentes pueden apropiarse de los fondos de las victimas. -

Como fue una investigación documental donde se analizo tanto doctrina como jurisprudencia e información oficial, se analizaron casos pertinentes para poder vislumbrar la importancia económica de estas estafas y el impacto en el país.

Posteriormente se analizó la responsabilidad penal y civil de los imputados por los distintos delitos, indicando cuales son los requisitos para poder ser sindicado como penalmente o civilmente responsable de una estafa informática. Para luego adentrarnos en el quid de la cuestión con respecto a quién responde por cuestiones penales, quién por civiles, la posibilidad de reclamar en ambas sedes, la constitución de actor civil, particular damnificado, la necesidad de aguardar sentencia penal o no y derecho comparado.

Por último, se avanzó sobre las problemáticas procesales civiles y penales. Analizando cuál es la búsqueda en cada una de ellas y que relación o dependencia tienen entre sí. Cuál es la situación de las víctimas, que opciones tienen y que podemos dejar planteado para el futuro con respecto a estos delitos y sus reparaciones.

Volviendo a la cuestión que interesa plasmar en esta investigación es la cuestión económica, resarcitoria, sus responsables y las diferentes vías de acción y quienes tienen la potestad.

En todos los casos analizados de sentencias civiles en casos de delitos informáticos se vislumbra que la entidad bancaria o billetera virtual es la figura pasiva de los reclamos civiles. Por lo que surge a nivel indemnizatorio su responsabilidad por el riesgo creado y la confianza depositada en ellas.

Lo novedoso aquí es que la entidad bancaria va a responder civilmente por un delito que no cometió y por el cual nunca se obligó. Si bien no se la condena por el delito propiamente

dicho se la hace civilmente responsable de afrontar los daños y perjuicios que ese delito ocasiono.

Amplio esto…en el caso de las compañías aseguradoras, por ejemplo, se encuentran citadas en garantía para responsabilizarse por el hecho que genero su asegurado por un delito culposo.

Aquí la entidad bancaria, que deberá afrontar el pago de los daños y perjuicios por la falta de seguridad, por su factor de atribución objetivo, podría iniciar un reclamo para repetir contra el imputado, cosa que no puede hacer la compañía de seguros cuando responde por daños y perjuicios por lo que ocasiono su asegurado.

El quid de la cuestión aquí está en la posibilidad que he planteado precedentemente de poder realizar reclamos por diferentes causas fuentes:

Aquí habría identidad de personas, pero el reclamo se fundaría en diferentes fuentes:

- Reclamo como víctima de estafa a la entidad bancaria por su deber de seguridad, vulnerabilidad del sistema.
- Reclamo al imputado penal por daños y perjuicios ya sea en sede penal o de manera independiente en sede civil. El juez penal no puede imponer de oficio indemnizaciones así que solo procede a petición de parte
- Asimismo, reclama la entidad bancaria al imputado penalmente responsable como víctima similar a una acción de repetición, ya que producto de su accionar ilícito se afectó su patrimonio y su imagen pública.
- Por último, habría que verificar en futuras investigaciones la potestad de las empresas aseguradora de las entidades bancarias la viabilidad de un reclamo al imputado/condenado penal.-

Entiendo que este mecanismo de reclamos en simultaneo podría desalentar a los delincuentes producto de que como hemos visto en las sentencias traídas a análisis son las entidades bancarias las que terminan solventando los daños al no poder responsabilizar penalmente a los imputados. Pero en el caso de que efectivamente se condene al imputado además de la pena de prisión desalentaría tener que desapoderarse de lo sustraído.

Así como podemos iniciar reclamos civiles en paralelo a las entidades bancarias podría la entidad reclamar al imputado para que procedan cautelares, para ser un agente activo de

investigación, que se continúen las averiguaciones hacia todas las personas que han recibido dinero y poder atacar el problema desde la raíz.

Evidentemente al ser un flagelo meramente económico no toma la dimensión de política criminal que debería alcanzar. Pensemos que el costo que tiene toda la operatoria bancaria se ve afectada por las circunstancias de tener que afrontar cada vez más frecuentemente indemnizaciones por daños y perjuicios o nulidades de contrato por delitos que no han cometido.

Poder implementar un procedimiento especial como se utiliza en el caso de Venezuela sería de gran agilidad para las entidades y para las personas estafadas. Pensemos en los casos en donde efectivamente encontremos un culpable, donde efectivamente podamos determinar quién ha perpetrado el delito, la distribución de ese dinero en diferentes cuentas, señalar los verdaderos responsables y no las llamadas "mulas". En ese caso tendríamos una persona determinada, un imputado encontrado culpable que debería reparar ese daño generado por la estafa.

La práctica indica que en los casos de estafas informáticas se realiza la denuncia penal como requisito por parte de la entidad bancaria pero luego no se persigue al delincuente, ya que a la víctima le interesa más la restitución de su dinero que la posible condena penal del imputado que muchas veces ni siquiera se puede ubicar.

Entonces la pregunta es que …¿Qué pasaría si las entidades bancarias iniciarán y continuarán todas las causas penales por las que deben abonar en sede civil? No podría cambiar el paradigma y evidenciar que las dichas entidades también son víctimas; que las personas que se vieron privadas de su dinero colaboraran en la investigación; ¿que la cuestión tomara un estado público y dejáramos las cifras negras por el marketing negativo que trae haber sido estafados?

El desafío de nuestra era será la prevención de estos delitos, pero también las sanciones ejemplares para desalentar estas prácticas. Que las entidades bancarias opten por el reclamo ante los delincuentes será mi desafío como profesional.

REFERENCIAS

Aboso, G. E. (2022). *Ciberdelitos : análisis doctrinario y jurisprudencial /...[et al.]; .* Ciudad Autónoma de Buenos Aires : : elDial.com Libro digital, EPUB.

Alferillo, P. E. (2015, 09 01). *La vinculación entre la acción penal y civil de daños en el Código Civil y Comercial.*

Alterini, A. A. (2008, 04 09). Las reformas a la ley de defensa del consumidor. Primera lectura, 20 años después. *Revista*. La Ley.

Anonimo compilado por Ricardo Antonio Parada; José Daniel Errecaborde. (2018). *Cibercrimen y delitos informáticos. .* ERREIUS.

Argentina.gob.ar. (2023, Octubre 14). From https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf,

Bertolino, P. (1998). *Código Procesal Penal de la Provincia de Buenos Aires Ley 11.922, comentado y concordado.* Ediciones Depalma Bs As.

Blanco Cordero I; Fabián Caparrós E.; Prado Saldarriaga V.; Santander Abril G. & Zaragoza Aguado J. . (n.d.). *Combate al Lavado de Activos desde el.* Quinta edición: Organización de los Estados Americanos – OEA.

Borghello, Cristian; Temperini, Marcelo G. I. (2012). Suplantación de Identidad Digital como delito informático en Argentina. *X Simposio Argentino de Informática y Derecho (SID 2012)*, (pp. 78-93). La Plata.

Bueres, Alberto y Zavala de González, Matilde, . (2016). *"Código Civil y Comercial de la Nación comentado", 2ª edición, Tomo II.* Buenos Aires: Editorial Hammurabi.

Buompadre, J. E. (2009). *Tratado de derecho penal. Parte especial.* Astrea.

Cavada Herrera, J. P. (2020). *Cibercrimen y delito informático:Definiciones en legislación internacional,nacional y extranjera.* Biblioteca del Congreso Nacional de Chile - Asesoria Parlamentaria.

Ciberseguridad, D. N. (2021). *Phishing Una guía para conocer sus modalidades y prevenirlas.* Jefatura de gabinete de ministros. Secretaría de Innovación Pública.

Código Penal de la Nación Argentina (CPNA). ((T.O. 1984 actualizado)). *LEY 11.179*. ARGENTINA.

Cuadernillo N°2: Ciberdelitos y estadas digitales. (2022). DNDCAC | COFEDEC.

Gianfelici, M. C. (1987). Responsabilidad civil emergente de la informática. *Revista*.

Guevara Alban, G., Verdesoto Arguello, A., & Castro Molina, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Recimundo, Revista cientifica Mundo de la investigación y el conocimiento*, pp. 163-173.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. . (2014). *Metodología de la investigación (6a. ed. --.).* . México D.F.:: McGraw-Hill.

Jefatura de Gabinete de Ministros, Secretaria de Innovación Pública. (2022). *Incidentes informáticos. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT.ar.* Buenos Aires. From https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f__0.pdf

Lejed Cona, J. A. (2022). Cuadernos de Derecho procesal penal. *Tribunal penal, indemnización civil y delitos informáticos. N 32 Serie Doctrina*. Venezuela.

Martínez, M. S. (2018). Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. In c. p. Anonimo, & J. D. Errecaborde, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet* (p. 33). Buenos Aires: Erreius.

Mosset Iturraspe, J. (2017). *"Responsabilidad civil", 4ª edición.* Buenos Aires: La Ley.

Paz Sefair, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. Revista de derecho Privado. 35 .

Pizarro & Vallespinos. (2018). *Tratado de Responsabiliad Civil , Tomo III.* Buenos Aires: Rubinzal Culzoni Editores.

Saín, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas. In c. p. Anonimo, & J. D. -, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet /* (p. 7). Buenos Aires: Erreius.

Stiglitz Gabriel A. ; Stiglitz Rosana M. . (1998). Responsabilidad civil por daños derivados de la informática. *Responsabilidad Civil Doctrinas Esenciales Tomo VI*. La Ley .

Temperini, M. (2018). Delitos informaticos y cibercrimen . In c. p. Anonimo, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet.* Erreius.

Vasquez Rossi, J. (2011). *Derecho Procesal Penal.* Rubinzal – Culzoni.

Yuni J.; Urbano. C. (2014). *Técnicas para investigar 2 (Vol. 2). [Versión electrónica].* Buenos Aires: Brujas.