revista pensamiento penal

Ciberfraudes en la Ciudad Autónoma de Buenos Aires

Análisis de la Capacidad Preventiva del Sistema Penal

Paula Garrido[1]

SUMARIO: I.- Introducción; II.- Conceptos y contexto; III.- Objetivos; IV.- Metodología; V.- Resultados; VI. - Discusión y conclusión; VII.- Referencias bibliográficas

RESUMEN: Este estudio pretende analizar el poder preventivo del sistema penal de la Ciudad Autónoma de Buenos Aires (CABA) en la República Argentina respecto del delito de estafa informática desde la perspectiva de la Escuela Clásica y sus variables de disuasión (certeza, celeridad y severidad). Para ello, la recopilación de datos incluye entrevistas con ocho actores clave del sistema penal de la capital de Argentina. Los resultados evidencian que la capacidad del sistema penal de CABA para prevenir estafas informáticas es limitada y que, si bien la pena en expectativa es severa, lo cierto es que no existe certidumbre de castigo y que la celeridad para arribar a un resultado condenatorio en estos casos es insuficiente.

PALABRAS CLAVE: Estafa informática – ciberfraude - escuela clásica – disuasión – prevención - Argentina

[1] Abogada por la Universidad de Buenos Aires (UBA) y Magíster en Criminología y Ejecución Penal por la Universitat Pompeu Fabra. Actualmente, se desempeña como Secretaria en el Juzgado Penal, Contravencional y de Faltas N° 25. Mail: pgarrido@jusbaires.gob.ar

I.- Introducción

El auge del uso de internet y las Tecnologías de la Información y Comunicación (TIC) han significado un cambio de paradigma en la sociedad y la forma de vincularse de las personas (Sosa, 2023). Gran parte de nuestras vidas transcurre en el ciberespacio, lugar en el que compartimos una enorme cantidad de información personal y que permite gestionar algunos asuntos vinculados con nuestro día a día.

El progreso tecnológico, el uso masivo de internet y la globalización dieron lugar a un nuevo mundo digital al que se trasladaron muchas de las características y conductas de la sociedad del plano físico al plano cibernético. De este modo, en el espacio virtual no solamente ha ido en aumento el uso de herramientas digitales para cuestiones de la vida diaria (redes sociales, cuentas bancarias, entre otros), sino que también se han incrementado los comportamientos delictivos cometidos a través de él. Este fenómeno es conocido como la ciberdelincuencia, es decir, aquellos delitos cometidos a través de Internet o para los que se utilizaron herramientas digitales para su comisión (Jewkes & Yar, 2010). Estas maniobras pueden ser de índole social, política o patrimonial (Miró Llinares, 2012), dentro del último grupo se encuentra comprendido el ciberfraude (en este trabajo, los términos "ciberfraude", "estafa informática", "ciberestafa", "fraude informático" y "fraude digital" serán utilizados como sinónimos).

Durante la última década, tal como señalan Arimatéia da Cruz y Godbee (2020), la República Argentina ha trabajado en la persecución de los delitos cometidos en y a través del ciberespacio de conformidad con lo establecido en el Convenio de Budapest[2]. Este avance ha sido fundamental ya que, a raíz de ello, se han tipificado en el Código Penal Argentino (CP) diversas conductas ilícitas. Dentro de este nuevo catálogo de delitos se incorporó la estafa informática, entendida como el uso de medios digitales para la adquisición delictiva de dinero o bienes de las víctimas mediante el uso de engaños (Miró Llinares, 2013; Holt et al., 2017), tipificada en el artículo 173 incisos 15 y 16 del CP[3].

[2] A fines del año 2017, Argentina adhirió, mediante la Ley Nacional 27.411 publicada en el Boletín Oficial el 15/12/17, al Convenio sobre Ciberdelitos del Consejo de Europa, firmado en la ciudad de Budapest en el año 2001. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm .

[3] El art. 173 en su inciso 15 del Código Penal fue introducido por la Ley Nacional 25.930 (disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/95000-99999/98807/norma.htm) y el inciso 16 del art. 173 del Código Penal incorporado por la Ley

La transición del fraude a los espacios online permite que el ciberdelincuente se dirija simultáneamente a una población masiva de potenciales víctimas en el mundo entero. Los efectos generados en las víctimas representan una gran amenaza, no solamente por las importantes pérdidas económicas sufridas, sino también por el impacto negativo a nivel emocional y psicológico (Kemp & Moneva, 2020; Palassis et al., 2021). Es importante mencionar que no existen datos registrados sobre estafas informáticas cometidas a lo largo de los años en Argentina[4] , por lo que no es posible describir las tendencias en la Ciudad Autónoma de Buenos Aires (de aquí en adelante, CABA). Sin embargo, es interesante señalar que, en el año 2021, las estafas informáticas se registraron como el ciberdelito más denunciado ante el fuero local de CABA -quien posee competencia para investigar estos hechos- y, además, ocuparon el quinto lugar dentro de los delitos con mayor número de casos ingresados al Ministerio Público Fiscal de CABA (en adelante, MPF) en ese mismo año, tal como se refleja en los siguientes gráficos:

Gráfico 1: Elaborado a partir de los datos publicados por el Gobierno de la Ciudad Autónoma de Buenos Aires en https://www.estadisticaciudad.gob.ar/eyc/?p=75692.

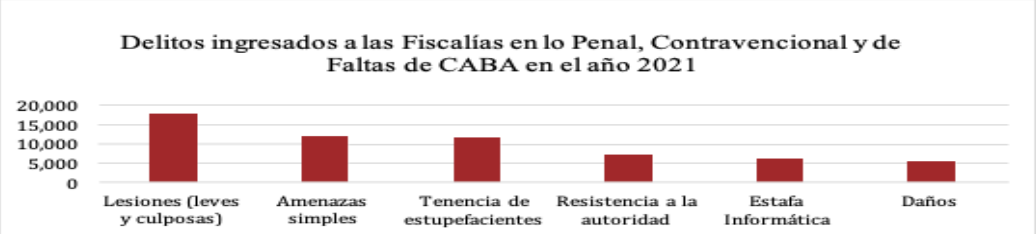

Gráfico 2: Elaborado a partir de los datos publicados por el Gobierno de la Ciudad Autónoma de Buenos Aires en https://www.estadisticaciudad.gob.ar/eyc/?p=75692.

Las estafas informáticas plantean una amenaza significativa para todos los países. A modo de ejemplo, España, de conformidad con el Informe sobre Cibercriminalidad del año 2021, en el periodo comprendido entre 2017 a 2021 constata el aumento de ciberdelitos. Particularmente, en 2021 registra un 6,1% más

Nacional 26.388 (disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000- 144999/141790/norma.htm)

[4] Se han buscado datos en Policía, Gobierno de la Ciudad de Buenos Aires, Ministerio de Justicia y Derechos Humanos y en el Ministerio Público Fiscal.

con respecto al año anterior y, dentro de esa cifra, el 87,4% corresponde a ciberfraudes. Es posible que tendencias similares se reflejen también en Argentina.

Frente a este panorama, el Poder Judicial de la CABA ha desarrollado nuevas formas de investigación y ha creado unidades especializadas para perseguir este tipo de delincuencia con el fin de aumentar la efectividad en la detección de estas conductas. Sin embargo, la proliferación de las conductas lesivas realizadas en el ciberespacio, caracterizadas por su dinamismo y variación continua, dificulta la tarea del sistema penal. La falta de conocimiento sobre los mecanismos de denuncia, la desconfianza de la sociedad en la capacidad del sistema penal para detener a los ciberdelincuentes, la volatilidad de las pruebas digitales, el reto legislativo para castigar la variedad de conductas que se realizan a través de la web y la carencia de recursos son algunas de las dificultades a las que se enfrenta el sistema penal a la hora de investigar estafas informáticas (Temperini, 2015; Holt et al., 2017; Dodge & Burruss, 2019; Kemp et al., 2020; De Paoli et al., 2020; Maimon, 2020). Los ciberdelincuentes tienen acceso a una amplia gama de herramientas que dificultan su persecución y, debido a la complejidad de los delitos cometidos en este entorno, las investigaciones resultan más desafiantes para quienes conforman el sistema penal (Cámara Arroyo, 2020). Los obstáculos mencionados pueden disminuir la efectividad preventiva del sistema penal.

El relevante aumento en la tasa de ciberestafas denunciadas en CABA junto con las consecuencias que sufren las víctimas de este delito incentiva a prestar atención al funcionamiento y respuesta que da el sistema penal (Policía, Juzgados y Fiscalías) a este fenómeno.

Este trabajo tendrá por objeto estudiar la capacidad preventiva del sistema penal actual de CABA en materia de ciberfraudes. Se analizarán las percepciones de algunos actores claves del sistema penal de CABA desde la perspectiva de la escuela criminológica clásica y las variables de la disuasión (certeza, celeridad y severidad). Este análisis del vínculo entre las percepciones del riesgo y el sistema penal es imperativo para comprender si el funcionamiento de la administración de justicia tiene efectos preventivos (Nagin, 2013).

En Argentina -y América Latina en general- la capacidad del sistema penal y policial para prevenir estafas informáticas no ha sido estudiada en profundidad[5]

[5] Se ha buscado en Google Scholar, Dialnet, La Ley y Scopus con las siguientes palabras claves: disuasión sistema penal ciberfraude Argentina, sistema penal y ciberfraudes CABA, prevención sistema penal Argentina, ciberfraudes y sistema penal en Argentina, prevention/deterrence cyber

como sí en otros países del hemisferio norte, tales como Estados Unidos o Inglaterra (por ejemplo, Levi et al., 2017; Holt et al., 2017; Bossler et al., 2019; Maimon, 2020; Cockcroft et al., 2021), cuya coyuntura difiere sustancialmente de la realidad sudamericana debido a las características intrínsecas de la sociedad y sus recursos económicos.

Es por este motivo que esta investigación, desde una óptica teórica, pretende nutrir y hacer un aporte al sistema penal local en materia de ciberestafas al realizar un análisis crítico de los mecanismos de prevención de estas conductas. Este estudio adquiere una gran importancia para la construcción del conocimiento en el área, ya que se trata de un campo que todavía no ha sido explorado en profundidad en Argentina y será cada vez más relevante en el ámbito del sistema penal. Además, proporciona a los integrantes del sistema penal la oportunidad de comprender las nuevas prácticas y mejorarlas.

II.- Conceptos y Contexto

a) Modelos preventivos de la pena y Escuela Clásica

El modelo preventivo-especial y preventivo-general de la pena consiste en utilizar al castigo como medio para que las personas no cometan delitos. La teoría de la prevención especial introducida por Von Liszt (1970, como se citó en Crespo, 1999) entiende que la finalidad de la pena consiste en hacer desistir al autor de futuros delitos, es decir que la sanción se dirige a persuadir a un autor individual. Según Roxin (1997), este tipo de prevención puede darse de varias formas: encerrando al delincuente para proteger al resto de la comunidad de esta amenaza, intimidando al autor al imponerle un castigo y evitando la reincidencia del delincuente mediante su corrección. La teoría de la prevención general, por su parte, considera que la pena no debe actuar de manera particular sobre el condenado, sino que debe apuntar de forma general sobre la comunidad (Roxin, 1997). La faceta negativa de la prevención general propuesta por Feuerbach (1989, como se citó en Miró Llinares & Ortuño, 2013) se da cuando la pena es la motivación general de la sociedad para la no realización de una conducta por medio de la amenaza con una sanción grave, mientras que el aspecto positivo tiene por objeto la interiorización de los valores jurídicos por parte de la sociedad y generar confianza en el ordenamiento

fraud Argentina, prevention of cyber fraud in the criminal justice system, cyber fraud deterrence CABA, deterrence Buenos Aires, prevention in the criminal justice system, criminal justice cybercrime Buenos Aires.

jurídico (Roxin, 1997). El modelo preventivo se vincula con los postulados de la Escuela Clásica y, a su vez, con la Teoría de la Elección Racional.

La Escuela Clásica responde a la lógica de la prevención general negativa. Su idea principal radica en buscar un mejor funcionamiento del derecho penal, partiendo de la base de que una amenaza de pena adecuada y eficaz lograría que los individuos no cometan delitos, por lo que las sanciones debían ser lo suficientemente duras como para disuadir de cometer delitos en el futuro a esa persona y al resto de las personas que presenciaran la sanción (Yar & Steinmetz, 2019).

Uno de los autores principales de la Escuela Clásica fue Beccaria (1738-1794). Este autor italiano parte de una idea utilitarista de las penas y afirma que el fin de la pena es impedir que el delincuente cause nuevos daños a la sociedad, así como también evitar que las demás personas de la comunidad cometan infracciones (Beccaria, 1968). A efectos de lograr que las penas sean preventivas, el autor refiere que deben imponerse con celeridad, toda vez que cuanto más rápido se imponga ese castigo mayor será el efecto que genere en el delincuente y en la sociedad, siendo que tomarán dimensión de las consecuencias de sus actos. Asimismo, Beccaria asegura que las penas deben ser certeras ya que la certidumbre de un castigo es lo que provocará temor en quien pretende cometer delitos y ello llevará a que desista de realizar el hecho delictivo. Finalmente, el autor sostiene que la pena debe ser severa, de modo que las consecuencias negativas del delito excedan sus resultados positivos. Además, Beccaria (1968) sostiene que la finalidad de las penas es prevenir los delitos e imponer castigos que causen un efecto más eficaz y duradero sobre la sociedad y menos dolor al delincuente, entendiendo a los seres humanos como seres racionales y considerando que los motores de la acción humana son el dolor y el placer (Larrauri & Cid, 2001).

La Teoría de la Elección Racional recoge las ideas de la Escuela Clásica, tal como señalan Larrauri y Cid (2001). Esta teoría sostiene que cometer un delito no es algo que se encuentre exclusivamente en un tipo de personas, sino que la probabilidad de cometer un delito es una característica común a todos los individuos, por lo que la elección de delinquir dependerá del balance entre costos y beneficios (Durlauf & Nagin, 2011; Miró Llinares & Ortuño, 2013). En otras palabras, el ser humano es libre y racional y la decisión de delinquir es una opción en la que el potencial delincuente pondera la rentabilidad que implica la realización de una conducta delictiva, por lo que los sistemas penales cumplen un rol fundamental a la hora de elevar los costos y reducir los beneficios de las conductas ilícitas (Durlauf & Nagin, 2011).

La disuasión penal es la prevención de actos delictivos mediante la amenaza de un castigo legal. El aspecto objetivo de la disuasión se da con la combinación de las variables certeza, celeridad y severidad, mientras que el aspecto subjetivo es aquello que los potenciales delincuentes creen que son los riesgos a los que se enfrentan al delinquir, cómo los perciben y también cómo ponderan esos riesgos respecto de los posibles beneficios que podrían obtener frente a una conducta ilícita (Bottoms & Von Hirsch, 2010). Al respecto, tal como sugieren Yar y Steinmetz (2019), la disuasión suele centrarse en los factores que influyen en la percepción del castigo en términos de certeza, severidad y celeridad.

b) Prevención penal de estafas informáticas

De acuerdo con lo manifestado en el apartado anterior, la disuasión penal es la prevención de hechos ilícitos mediante la amenaza de un castigo (Bottoms & Von Hirsch, 2010). Para que los castigos impuestos generen efectos preventivos, las penas deben ser certeras, severas y deben imponerse con celeridad (Larrauri & Cid, 2001). La disuasión es la respuesta en el comportamiento a la percepción de amenazas de castigo y sanción (Nagin, 2013).

La severidad del castigo exige que la pena exceda el bien esperado al cometer una conducta ilícita (Larrauri & Cid, 2001). Al respecto, la pena prevista para el delito de estafa es de un mes a seis años de prisión y dependerá del juez establecer (dentro del mínimo y el máximo determinado por el CP) la pena aplicable en cada caso según las características del hecho. La severidad de las penas se encuentra -hace ya varios años- en la agenda política de Argentina en razón de la creencia popular de que los castigos deben ser más duros (Fuentes, 2004)[6].

El concepto de celeridad es importante en el marco de la investigación de estafas informáticas ya que cuanto más rápido se imponga el castigo, más efecto tendrá en el potencial delincuente y en la asociación de que los actos tienen consecuencias. Sin embargo, en el plano del mundo digital, la investigación de los ciberfraudes es particularmente compleja debido al tiempo que implica obtener la evidencia necesaria para condenar a una persona que cometió una estafa en la web y

[6] Ver también: https://elpais.com/internacional/2017/05/16/argentina/1494951468_406639.html y Raggio, S & Cipriano García, R. (2023). Las consecuencias sociales de la mano dura en la Argentina. *CLACSO - Consejo Latinoamericano de Ciencias Sociales| Conselho Latino-americano de Ciências Sociais*. https://www.clacso.org/las-consecuencias-sociales-de-la-mano-dura-en-la- argentina/

la intangibilidad y transitoriedad de esa evidencia (Sosa, 2023; Temperini, 2015; Yar & Steinmetz, 2019; Maimon, 2020; Whelan & Harkin, 2021).

La alta probabilidad de aprehensión por parte de las autoridades, la probabilidad de enjuiciamiento y la probabilidad de obtener una condena son las principales causas de la disuasión penal (Nagin, 2013).

Los estudios criminológicos[7] tienden a mostrar correlaciones estadísticamente significativas entre la certeza del castigo y los índices de delincuencia (Bottoms & Von Hirsch, 2010). Si bien el aspecto objetivo de la disuasión penal se compone de tres variables, desde la criminología, la evidencia a favor del efecto preventivo de la variable certeza del castigo es mucho más consistente que las demás, es decir que la certidumbre de obtener un castigo al realizar una conducta ilícita resulta el componente disuasorio más eficaz, y esto se aplica también al ámbito cibernético (Holt et al., 2017).

La decisión de cometer una infracción está vinculada a la evaluación de riesgo de ser sancionado, lo cual es de suma importancia para el sistema penal. Las políticas criminales deben enfocarse en detectar la mayor cantidad de infracciones y sancionar a quienes las cometen. Cabe mencionar aquí lo expuesto por Larrauri (1998), quien sugiere que el sistema preventivo general no ha sido demostrado empíricamente y que corresponde, además de realizar un análisis de las consecuencias que implica la imposición de un castigo, evaluar también la existencia de factores de otro tipo (sociales, culturales, económicos) que influyan de modo directo en la prevención de delitos.

Es posible trasladar el concepto de prevención penal al mundo del ciberespacio. Sin embargo, en atención a las propias características de la web, el plano virtual reviste algunas dificultades que entorpecen el efecto preventivo del sistema penal. Los parámetros espacio- temporales, el anonimato y la transnacionalidad de las conductas ilícitas cometidas mediante medios digitales inciden en las dificultades de persecución jurídico-penal de las estafas informáticas (Miró Llinares, 2012; Yar & Steinmetz, 2019).

[7] Los principales estudios de asociación fueron realizados por David Farrington en 1994 y 1998. Dichos estudios muestran una relación estadística significativa entre la probabilidad de detención y condena y la incidencia de la delincuencia (Bottoms &Von Hirsch, 2010).

Larrauri (2018) sugiere que, si bien se habla de prevención del delito, lo cierto es que sería más adecuado hablar de reducción de la delincuencia, ya que en realidad las sociedades aspiran a reducir la delincuencia y no a prevenirla totalmente.

Varios estudios indican que la teoría de la disuasión con relación a los ciberdelitos carece de una base sólida debido a la escasez de investigación empírica sobre el tema. Además, se considera que este tema es complejo y requiere un enfoque interdisciplinario para comprender su efectividad (Holt et al., 2017; Maimon, 2020; Castro Toledo, 2021; Gómez Bellvís et al., 2023). Sin embargo, todos estos estudios coinciden en que la certeza de ser aprehendido, incluso en el ámbito virtual, es la variable más relevante.

La eficacia de las estrategias basadas en la disuasión para prevenir y mitigar los delitos cometidos *online* es más bien desconocida en el ámbito del derecho y la política (Maimon, 2020), por lo que resulta interesante evaluar el rol que cumple el aparato jurídico-penal y policial en la persecución y seguimiento de estos comportamientos.

c) Estafas Informáticas: legislación en Argentina

El fraude es la adquisición delictiva de dinero o bienes de las víctimas mediante el uso del engaño o la trampa (Holt et al., 2017; Bossler et al., 2019; Miró Llinares, 2021). Esta figura descubrió en el ciberespacio un nuevo ámbito de oportunidad criminal (Miró Llinares, 2011) y se trata, entonces, de conductas que coinciden en lo esencial con el fraude tradicional, pero que para su configuración requieren una comunicación posible en internet, ya que se consuma a través de medios digitales (Miró Llinares, 2022). En la mayoría de los casos, el ciberfraude se caracteriza por ser una forma de delincuencia organizada que involucra a tres o más personas y, dentro de esa organización, se pueden identificar dos tipos: aquellos con estructuras jerárquicas, con cierto grado de centralización, división del trabajo y líderes identificables, y aquellos que operan como redes transitorias, sin una estructura clara, de forma horizontal, sin una organización fija y descentralizada (Maras, 2022).

Argentina incluyó[8], con la entrada en vigor de las Leyes Nacionales 25.930 y 26.388, un catálogo de figuras delictivas vinculadas a los delitos informáticos (Garat

[8] A raíz del Convenio sobre Ciberdelincuencia de Budapest, el cual establece que se entiende por fraude informático "a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno

& Reale, 2022). De este modo, se incorporó la estafa informática al artículo 173 del Código Penal:

"15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos."

La pena prevista para estas modalidades de estafa es la misma que para la figura tradicional: de un mes a seis años de prisión. La incorporación de las maniobras fraudulentas que involucran sistemas informáticos al CP intenta dar respuesta a las exigencias del Convenio sobre Ciberdelincuencia de Budapest[9] y, asimismo, a algunas situaciones patrimoniales abusivas relacionadas con la informática, por ejemplo, aquellas cuestiones relacionadas a la utilización de máquinas y mecanismos digitales para la maniobra de estafa[10] cuya utilización dificultaba encuadrar la maniobra dentro de la conducta típica de estafa tradicional (Linares, 2020; Miró Linares, 2021).

La diferencia entre la estafa tradicional (prevista en el artículo 172 del Código Penal[11]) y la digital es que el engaño se reemplaza por la manipulación de los medios informáticos y/o de las tarjetas de crédito y débito, lo que finalmente deriva en un perjuicio patrimonial (Balcarce & Arocena, 2020; Martínez, 2018; Simaz et al., 2020).

mismo o para otra persona.". Convenio disponible para su consulta en https://rm.coe.int/16802fa403.

[9] El artículo 8 del Convenio de Budapest establece que cada estado parte deberá adoptar las medidas legislativas -o de cualquier otro tipo- que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante la alteración de datos informáticos o cualquier interferencia informática con intenciones fraudulentas.

[10] Linares (2020) sugiere que la tipificación de estas figuras en el Código Penal permite superar los problemas vinculados a la imposibilidad de estafar a una máquina u ordenador y, de esa manera, eliminar posibles planteos de atipicidad que se daban por no darse la secuencia tradicional de la estafa.

[11] Artículo 172 del Código Penal Argentino: "*Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión,empresa o negociación o valiéndose de cualquier otro ardid o engaño.*".

d) Estructura del sistema penal de CABA y su relación con la investigación de estafas informáticas

Previo a adentrarme en la descripción de CABA, resulta necesario mencionar que el sistema penal está integrado por las fuerzas policiales, del poder judicial y del sistema de penas, cuya finalidad es prevenir y perseguir la delincuencia (Larrauri, 2018).

Argentina adopta para su gobierno la forma representativa, republicana y federal: republicana debido a que se basa en la división, control y equilibrio entre los tres poderes (legislativo, ejecutivo y judicial) y federal porque cada Provincia conserva su autonomía.

De este modo, cada una de las Provincias que integran la Argentina cuenta con su propio Poder Judicial y un sistema policial-penal autónomo para perseguir los delitos establecidos en el CP, tal como es el caso de la CABA con el fuero Penal, Contravencional y de Faltas.

El artículo 107 de la Constitución de la Ciudad de Buenos Aires[12] establece que el Poder Judicial local se compone de cuatro órganos, entre los que se encuentran los Tribunales y el Ministerio Público Fiscal. Además, del MPF depende el Cuerpo de Investigaciones Judiciales (CIJ)[13], también conocida como Policía Judicial, cuyo objeto es la investigación de los delitos, la individualización de los autores y partícipes del hecho que se investiga y la obtención de pruebas útiles para el caso. Es importante destacar que en CABA rige el principio acusatorio adversarial. Esto implica que la responsabilidad de la investigación recae en el MPF, que recibe las denuncias, presenta la acusación pública y lleva a cabo las diligencias necesarias para esclarecer el delito. El juez, por su parte, limita sus funciones a ejercer control jurisdiccional, es decir, su labor consiste en analizar las evidencias presentadas por la fiscalía o la defensa y no se encuentra habilitado para solicitar medidas de prueba que no sean expresamente requeridas por las partes, pues la idea es que conserve su imparcialidad.

[12] Artículo 107: "*El Poder Judicial de la Ciudad lo integra el Tribunal Superior de Justicia, el Consejo de la Magistratura, los demás tribunales que la ley establezca y el Ministerio Público.*". Ver en: http://www.infoleg.gob.ar/?page_id=166

[13] Creado por la Ley 2896 de la Ciudad Autónoma de Buenos Aires. Disponible para su consulta en: https://ar.vlex.com/vid/ley-n-2896-44696598.

En cuanto a la investigación de estafas informáticas, dentro del MPF y del CIJ existen equipos especializados para la pesquisa de este tipo de delitos[14], cuya tarea es recolectar, conservar, analizar y procesar la evidencia digital. Por su parte, los tribunales penales del fuero Penal, Contravencional y de Faltas, no cuentan con equipos especializados en ciberdelincuencia.

Es importante mencionar que la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI)[15] posee competencia para investigar ciberdelitos[16] y concentra la coordinación y dirección de todos los recursos humanos y materiales que el MPF de CABA destina a la investigación de los delitos y contravenciones informáticas[17].

El impacto del sistema penal para investigar estafas informáticas e individualizar a los autores y condenarlos podría resultar clave a los efectos de disuadir potenciales ciberdelincuentes. Para medir la capacidad del aparato jurídico-penal de la CABA en el desestimulo de estafas informáticas es necesario realizar un análisis de las dificultades a las que se enfrentan los operadores del sistema penal y su idoneidad para sortear los obstáculos que se presentan a la hora de llevar a cabo las pesquisas, así como también la efectividad para investigar, detectar, acusar y

[14] Dentro del CIJ existe la Unidad de Cibercrimen e Investigaciones Complejas, mientras que dentro del MPF se creó la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI).

[15] Creada mediante la Resolución 20/2020 de la Fiscalía General de la CABA.

[16] La resolución 20/2020 del MPF de CABA (acceder a https://mpfciudad.gob.ar/storage/archivos/Resoluci%C3%B3n%20FG%20N%C2%BA%20020-20.pdf) le asigna a la UFEDyCI competencia para investigar los siguientes delitos: estafa informática (art. 173 inciso 16 del CP), pornografía infantil (art. 128 del CP), "*Grooming*" o ciberacoso sexual infantil (art. 131 del CP), acceso sin autorización a un sistema (art. 153 del CP), daño informático simple y agravado (art. 183 y 184 del CP). En cuanto a las estafas informáticas, la competencia también le fue asignada al fuero local por ley en los términos del art. 2 de la Ley 24.588 ("Ley Cafiero") en cuanto asigna al fuero PCyF la competencia de los delitos que se establezcan en lo sucesivo (como es el caso de las estafas previstas en el art. 173 incisos 15 y 16) y conforme los precedentes N° 6397/09 'NN s/ inf. art. 00', del 27/08/09, nº 322174/2022 "Le Pain Quotidien", de 14/12/2022 y N° 7312 'Neves Canepa', de 27/12/10, entre otros, del Tribunal Superior de Justicia (máxima autoridad judicial local en todas las cuestiones de competencia no federaes, según la Corte Suprema de Justicia de la Nación conforme fallos 342:509).

[17] Además, esta unidad tiene la función de capacitar a los operadores del sistema judicial y brindarles herramientas para investigar ciberdelitos, profundizar mecanismos de cooperación internacional, brindar asesoramiento sobre evidencia digital e investigación y proceder de manera coordinada con las distintas fuerzas especializadas.

condenar a quienes cometieron fraudes informáticos. Es fundamental comprender cómo contribuyen los intervinientes especializados en la materia para hacer frente al fraude en línea (Bossler et al., 2020).

III.- Objetivos

A raíz de los antecedentes teóricos referidos en los apartados anteriores y teniendo en cuenta el evidente aumento en las denuncias registradas por estafas informáticas, el objetivo general del presente trabajo es analizar la capacidad preventiva del sistema penal de CABA en materia de ciberfraudes y, con base en este análisis, proponer recomendaciones y posibles mejoras.

Por su parte, los objetivos específicos de este trabajo son: i) distinguir las dificultades que enfrenta el sistema penal de CABA en la investigación del ciberfraude y la detección de ciberdelincuentes, ii) identificar si el sistema penal cuenta con herramientas que incrementen la probabilidad de detección de estafas informáticas y la eventual sanción de los autores y iii) analizar la capacidad del sistema para actuar de conformidad con las variables (certeza, celeridad y severidad) de la disuasión penal.

IV.- Metodología

a) Diseño de investigación

A fin de alcanzar los objetivos previamente enumerados, se utilizó el método cualitativo ya que permite profundizar el conocimiento sobre el objeto de estudio en el contexto en el que se da y desde la perspectiva de los actores intervinientes, utilizando métodos enfocados en la comunicación y observación de los fenómenos estudiados (Maxfield, 2014; Martí, 2018).

La elección de la metodología de investigación se determinó en función del fenómeno a investigar y con la finalidad de comprender el funcionamiento del sistema penal. La elección del método cualitativo en este estudio resultó conveniente para poner a la vista las dificultades a las que se enfrentan los operadores de la justicia y del personal policial a la hora de investigar fraudes digitales y estudiar la capacidad preventiva del sistema penal de CABA en estos casos. El diseño cualitativo está ligado, básicamente, a las entrevistas, los grupos de discusión, y la observación. Por ese motivo, para la realización del estudio se hicieron entrevistas con profesionales que desarrollan su actividad laboral en el ámbito del sistema penal de la Ciudad Autónoma de Buenos Aires.

El criterio de selección de la muestra no fue probabilístico sino intencional con el fin de obtener una muestra que incluya a los distintos actores que intervienen en los procesos judiciales. Se consideraron a los profesionales que ejercen actualmente cargos en CABA en las distintas categorías que componen el servicio penal en materia de investigación de estafas informáticas, así como también un abogado que se encuentra en ejercicio de la profesión como defensor de entidades bancarias en casos en los que se investigan estafas informáticas.

El acceso a los profesionales se efectuó mediante comunicación telefónica y/o mediante *Whatsapp*, oportunidad en la que se les informó sobre los objetivos del estudio, la modalidad de los encuentros y el anonimato de la información. En dicha ocasión, se les propuso una entrevista virtual por medios telemáticos[18], en razón de la imposibilidad de viajar a Argentina para realizar las entrevistas de manera presencial.

b) Participantes

La muestra de profesionales participantes en el estudio está integrada por 8 personas, distribuidas de la siguiente manera: 1 juez titular de un Juzgado Penal, Contravencional y de Faltas de la CABA, 1 operador (con cargo de Prosecretario Coadyuvante) de un Juzgado Penal, Contravencional y de Faltas de la CABA, 1 fiscal a cargo de la UFEDyCI, 1 operador (con cargo de Secretario) de la UFEDyCI, 2 integrantes de la Policía Judicial -CIJ-, 1 integrante de la Policía de la Ciudad y 1 abogado en ejercicio de su profesión.

Esta selección de participantes permite considerar las diversas perspectivas derivadas de los roles que desempeñan los entrevistados. Más precisamente, la selección permite analizar el punto de vista de quienes llevan adelante las investigaciones (operadores judiciales), así como también la percepción de quienes adoptan las decisiones y son los encargados de valorar la prueba y/o imponer una condena (jueces/fiscales), quienes se encargan de recibir las denuncias y realizar medidas probatorias (policía/CIJ) y, finalmente, un abogado que utiliza el servicio de justicia y tiene contacto directo con agentes externos.

c) Recolección de información

[18] Las entrevistas se realizaron a través de la aplicación *ZOOM*.

Con el fin de obtener datos empíricos, la recolección de información se ha realizado mediante entrevistas semi-estructuradas[19]. Este tipo de entrevistas da lugar a la incorporación de nuevas preguntas en caso de ser necesario, explicar las preguntas formuladas, pedir aclaraciones (Gutiérrez, 2021), y se adaptan a la dinámica de cada conversación y permiten profundizar en los aspectos significativos abordados por los entrevistados (Maxfield, 2014; Martí, 2018).

Las entrevistas se realizaron a partir de un guion de preguntas abiertas compuesto por cuatro bloques: i) denuncias, ii) investigación, iii) condenas y iv) evaluación global. Este guion de preguntas no se siguió de manera rígida, por lo que las personas entrevistadas no respondieron las mismas preguntas siguiendo un mismo y único orden, sino que la secuencia de entrevista se adaptó a la dinámica de la conversación. Se priorizó la espontaneidad y la libertad para responder, dando lugar a una charla descontracturada.

Los participantes fueron informados previamente sobre la grabación y el anonimato de las entrevistas, por lo que prestaron su consentimiento de manera oral al comenzar la conversación. Las entrevistas realizadas fueron grabadas y posteriormente transcritas mediante herramientas digitales.

A efectos de realizar un análisis comparativo -y ordenado- de los datos obtenidos en cada caso, creamos 8 categorías para codificar la información con el propósito de lograr los objetivos de esta investigación: i) incremento de denuncias; ii) cifra negra inferida; iii) dificultades percibidas; iv) capacitación del personal interviniente; v) recursos disponibles; vi) extensión de la investigación; vii) resolución de casos y viii) percepciones sobre la normativa vigente.

V.- Resultados

a) Incremento de denuncias

Todos los entrevistados coincidieron en que los últimos años se percibió un gran aumento en la cantidad de denuncias y casos de ciberfraudes que ingresaron a conocimiento del sistema penal. Al respecto, el policía entrevistado refirió: "*[...] el*

[19] La autora posee grabaciones el video y las respectivas transcripciones de las entrevistas realizadas, las cuales están disponibles para su consulta por cualquier persona interesada.

primer trimestre del 2022, si mal no recuerdo, en comparación con el 2021, había crecido aproximadamente un 200% la cantidad de hechos.".

Los entrevistados coinciden, además, en que desde el año 2020 debido a la pandemia mundial por COVID19, hubo un aumento descomunal de las denuncias por fraudes cometidos a través de la web. En este sentido, la fiscal sostuvo que *"La pandemia abrió ese grifo como para realmente permitir a los ciberdelincuentes a cometer más delitos relacionados con esta conducta" y*, por su parte, uno de los integrantes del CIJ (1) expresó que *"Cuando sucedió lo de la pandemia teníamos un diagrama de casos establecidos, teníamos un flujo de casos de cómo los trabajábamos y demás, y de golpe eso hizo pac y pasamos, no sé, de tener…cien casos a quinientos*"

Los operadores del juzgado y de la fiscalía señalaron que el delito previsto en el artículo 173 del CP es el ciberdelito más denunciado en la CABA, particularmente el representante del MPF manifestó que:

"[...] en los fraudes necesariamente quien hace la denuncia es una persona afectada por ese delito, ¿sí? O sea, hay un particular damnificado que va a la comisaría hace la denuncia, llama por teléfono al MPF hace la denuncia o manda un mail y hace la denuncia, [...], te diría de las que son instadas por denuncias de damnificados particulares, sí por lejos es el delito más denunciado de los ciberdelitos que nosotros tenemos competencia."

El abogado de entidades bancarias atribuyó el aumento de denuncias no sólo a la pandemia y la digitalización que la cuarentena implicó, sino a que actualmente los bancos te exigen la denuncia penal para proceder al reclamo administrativo y la devolución del dinero: *"La mayor parte de los bancos piden que se haga un tipo de denuncia penal, no una exposición civil, no un reclamo administrativo, sino una denuncia formal penal".*

b) Cifra negra inferida

Los participantes de esta investigación coincidieron en que los hechos delictivos no reportados a las autoridades en el caso de las estafas informáticas existen e infieren que la cifra debe ser alta. Por su parte, el operador del juzgado agregó que la tentativa de estafa informática nunca es denunciada, mientras que el trabajador de la fiscalía refirió:

"Yo creo que solo intervenimos en una porción mínima porque deben estar pasando muchas cosas que nosotros ni conocemos y que las terminamos conociendo solo porque la víctima necesita recuperar el dinero y termina utilizando el sistema penal como una pasarela o como un medio para conseguir su fin".

Algunos atribuyeron la cifra negra a que la gente no sabe cómo denunciar, pese a que últimamente se han intentado difundir los canales de denuncia (fiscal y operador juzgado). También atribuyen la existencia de la cifra negra a que los ciudadanos *"no creen en la justicia, entonces prefieren no denunciar"* (fiscal) o a que algunas personas creen "*que no tiene sentido con los tiempos en la justicia iniciar un caso con todo lo engorroso que puede ser"* (CIJ2).

El abogado refirió que la cifra negra era aún mayor antes de la pandemia porque los reclamos se resolvían directamente por vía administrativa cuando el banco devolvía el dinero, pero que ello se modificó debido a que ahora el banco exige una denuncia penal para continuar con el reclamo. Por otro lado, el operador del MPF dijo que, hasta el momento, no se habían registrado denuncias realizadas por entidades bancarias. Sobre este punto, el abogado manifestó que *"Si bien hoy en día hay más factores que llevan a los bancos a denunciar, no todos los hechos se denuncian, sino que hay un análisis específico según cada caso particular"*.

Además, los entrevistados señalaron que existe una especie de cifra negra que corresponde a los que sí hacen la denuncia, pero luego no quieren continuar porque el banco ya devolvió el dinero (CIJ2).

c) Dificultades percibidas

En varias entrevistas se resaltó que la mutación constante de las maniobras empleadas por los ciberdelincuentes para realizar este tipo de conductas es una gran dificultad a la hora de investigar los hechos. En este sentido, el secretario de la fiscalía señaló que *"Cuando yo creo que descubrí una maniobra o un tipo de maniobra y creo que ya la conozco bien aparece una maniobra nueva"*. Uno de los integrantes del CIJ (2) coincidió y dijo *"Creo que nuestra mayor dificultad es estar a la altura o al nivel de los delincuentes cibernéticos que todo el tiempo van mutando"*. Por su parte, la fiscal señaló que*:*

"[...] las modalidades cambian y mutan porque se sofistican. Con lo cual yo creo que una vez que el delincuente se ve que ese camino ya está, digamos, detectado por los investigadores buscan otro, ¿sí? Y siempre te da la sensación que uno va corriendo detrás de eso, ¿no? No adelante, sino detrás."

La variación de las conductas se relaciona, asimismo, con la utilización de herramientas innovadoras (TOR, telegram, VPN, entre otros) que aumentan el anonimato y dificultan el acceso a los datos de las personas que participaron de la estafa, tal como mencionaron algunos de los entrevistados (abogado, trabajador MPF).

Dos de los entrevistados (CIJ1 y trabajador MPF) señalaron que existe poca comunicación entre las distintas jurisdicciones de Argentina y que no tener una base de datos para poder cruzar la información obtenida en las distintas investigaciones realizadas resulta un inconveniente a la hora de investigar fraudes informáticos y no permite avanzar rápidamente en la recolección de información.

El policía manifestó que: *"La cantidad de estafas que hay son muchas, y la cantidad de personal que hay no llega a cubrir la necesidad de poder darle el tratamiento a cada una de las causas"*.

El personal del tribunal dijo que el tiempo que implica la investigación y recolección de evidencias en casos de ciberestafas es también una dificultad porque *"Cuando te llega la denuncia el delito ya fue consumado, el dinero ya fue gastado [...] y ya está todo terminado"*. Esto se relaciona con lo que surge de las entrevistas realizadas al policía y al secretario de la fiscalía, quienes manifestaron que una vez que el dinero se transfiere a billeteras virtuales o criptomonedas es muy difícil continuar la investigación, por lo que resulta fundamental intervenir tempranamente.

d) Capacitación del personal interviniente

Hemos encontrado que respecto a la capacitación y la preparación para investigar estafas informáticas existen respuestas totalmente opuestas según el lugar en el que trabajan los entrevistados. De este modo, de las entrevistas realizadas a los integrantes del MPF, del CIJ y la policía destaca principalmente que todos ellos se consideran capacitados y preparados para investigar los delitos aquí objeto de estudio. Incluso, el abogado manifestó que su experiencia con el personal de la UFEDyCI siempre fue excelente y que *"están muy bien preparados para investigar estos delitos"*. Sin embargo, todos ellos refirieron que no existen capacitaciones obligatorias dentro del MPF y que todo depende de la práctica adquirida con los casos que ingresan al sistema y *"de cada uno y de lo que quiera aprender"* (CIJ2).

Por su parte, el operador del juzgado reconoció no tener capacitación suficiente a pesar de estar interesado en la temática y, respecto del sistema penal, refirió *"Creo que no, no está capacitado a los niveles que hoy debería y que hoy te exige el fraude informático."*. El juez dijo que los conocimientos informáticos que tiene se deben a que creció utilizando la web y que el personal que integra su juzgado es gente joven que:

"Más o menos se da manía y lo que no nos damos manía o lo que no por ahí lo que nos excede mucho que en realidad no lo ha habido bueno o sea no en general más o menos como que lo

vamos lo vamos dilucidando y lo que no como que lo buscamos, está en la red está todo está en la red".

El secretario del MPF manifestó que existe una diferencia entre la capacitación del personal que compone el juzgado y el personal de la fiscalía:

"[...] nosotros como fiscalía damos por sentado un montón de conceptos y por ahí vos haces una petición al juzgado y desde el juzgado no lo entienden, no porque tengan mala predisposición ni nada, sino que por ahí nosotros empezamos a hablar en un lenguaje tan particular o tan técnico porque todo lo ciber te lleva a eso a convertirte a convertirte o a tener un perfil más técnico de interpretación de ciertos datos, eh, y esas diferencias a veces se notan".

e) Recursos disponibles

Respecto de los recursos disponibles para investigar estafas informáticas, los entrevistados coincidieron en que tanto el CIJ como la Policía de la Ciudad (principales encargados de recabar evidencia e investigar) cuentan con buenas herramientas tecnológicas para investigarlas, protocolos para obtener la prueba y conservarla para ser presentada en el expediente judicial. Incluso señalaron que existen unidades específicas como el laboratorio forense, unidades de ciberpatrullaje, entre otras. Uno de los entrevistados señaló *"[...] desde el punto de vista de los "fierros", como dicen los peritos, de la aparatología para poder hacer pericias, el CIJ está muy avanzado"* (operador MPF).

Algunos de los entrevistados hicieron saber que existe una diferencia entre los recursos tecnológicos y los recursos humanos: si bien el personal que interviene en la recolección de evidencia está capacitado para hacerlo, hay poco personal en relación a la cantidad de casos que ingresan a conocimiento del sistema penal. El policía manifestó que "*La cantidad de estafas que hay son muchas, y la cantidad de personal que hay no llega a cubrir la necesidad de poder darle el tratamiento a cada una de las causas",* comentario que coincide con lo referido por el integrante del CIJ (2), quien hizo saber que: "*Siempre el pedido es constante de gente porque se necesita y también porque el tiempo de capacitación es mucho más extenso que capaz en algún otro tipo de unidad".*

f) Extensión de la investigación

Sobre la duración de las investigaciones advertimos grandes diferencias en las percepciones de los entrevistados. Así, el operador del juzgado dijo que son casos muy lentos y que si la causa llega a juicio puede demorar "*tres, cuatro años tranquilamente"* en resolverse. Por su parte, la fiscal refirió que la investigación demora

"*meses, a lo sumo un año" y* uno de los integrantes del CIJ (2) aseguró que hay casos que "*ya tienen un año en proceso".*

Cabe destacar que los entrevistados refirieron que el tiempo de duración de una investigación y el ritmo al que se investigue depende de los agentes externos:

"En lo que es estafa dependemos mucho de los bancos de la información que ellos dan y en el tiempo que dan. Hay bancos que te pueden brindar la información en una semana y hay otros que actualmente están tardando 6 meses en darte la información. Eso para nosotros es un tiempo muerto, perdido de 6 meses que recién ahí podemos arrancar la investigación con lo que nos da el banco que son, digamos, los documentos básicos iniciales para arrancar una investigación de estafa." (CIJ2).

g) Resolución de los casos

El juez entrevistado manifestó no haber realizado juicios por estafas informáticas y que, si alguna vez impuso algún tipo de condena por este delito, fue por juicio abreviado (acuerdo de partes donde el autor del hecho reconoce el delito endilgado y negocia la pena que se le impondrá[20]). El operador del juzgado dijo que recordaba una única condena por un caso de ciberfraude debido a una maniobra "*bastante grande como para llegar a condena"* y que el tiempo de prisión impuesto no fue de efectivo cumplimiento, sino en suspenso. Además, refirió que son pocos los casos que llegan con requerimiento de juicio al juzgado. El abogado dijo que en su experiencia con estos casos vio únicamente una o dos condenas y que "*la mayor parte de los casos se resuelven con algún tipo de medida de extinción de la acción penal",* como suspensión del proceso a prueba (permite suspender el proceso penal contra el acusado a cambio de cumplir determinadas condiciones durante un período de prueba establecido y no requiere reconocimiento del hecho[21]).

El empleado del MPF dijo "*el año pasado hicimos unos 30 y pico de allanamientos en fraudes y condenas cerramos tres"* y que, en general, la forma de finalizar este tipo de causas es con reparación integral del daño o con suspensión del proceso a prueba. Destaca, además, que nunca fueron a juicio por un caso de ciberestafa y que las condenas registradas por la fiscalía especializada "*fueron cibermuleros, las cerramos porque eran, eran mulas que habían movido mucho dinero y que tenían conocimiento real de que estaba*

[20] Tal como establece el artículo 278 del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. Disponible en: https://www.argentina.gob.ar/normativa/provincial/ley-2303-123456789-0abc-defg-303-2000xvorpyel/actualizacion.

[21] Según artículo 76 bis del Código Penal Argentino.

pasando el dinero por sus cuentas", por lo que no cuentan con condenas impuestas a quienes se quedaron con el dinero y planificaron las maniobras.

Los integrantes del CIJ señalaron que quedan muchos casos sin resolver a pesar de que la fiscalía siga adelante con una imputación:

"*[…] si la fiscalía le imputa la primera cuenta [...] o el primer eslabón al que se recibe la plata y con eso la Fiscalía condena a alguien, digamos, por ahí el caso está resuelto. Para la Fiscalía. Para mí, como investigador creía que no."*

h) Percepciones sobre la normativa vigente

Los integrantes del tribunal refirieron que la pena establecida en el CP para los casos de estafas informáticas es acorde al catálogo de penas allí establecido. El juez dijo que es correctoel mínimo de la pena para casos de menor gravedad y que "*tenés hasta seis años para evaluar casos más graves."*

El secretario de la fiscalía se mostró de acuerdo con ello, pero manifestó que existe un problema en la redacción del tipo penal debido a que identificar los elementos del tipo penal con la redacción actual resulta dificultoso y que sería ideal *"que esté legislado como está legislado en el ordenamiento español, ya que te habla de transferencias inconsentidas, cosa que nuestro inciso dieciséis no lo dice, sino que solo habla de estafas informáticas".*

La fiscal y el policía, por su parte, refirieron que la pena debería ser más alta. La representante del MPF justificó su postura diciendo que la estafa tiene un alcance *"disruptivo, el alcance que tiene una persona desde su casa con la posibilidad de atacar 15, 20, 25 personas a la vez"* y que, además, debería considerarse reformar el Código de Procedimiento a fin de que se incorporen medios de investigación necesarios para estos casos.

VI.- Discusión y conclusión

Los hallazgos obtenidos en este estudio nos permiten elaborar conclusiones relevantes sobre los objetivos establecidos.

Respecto del primer objetivo específico, el cual hacía referencia a las dificultades que enfrenta el sistema penal de CABA en la investigación del ciberfraude, cabe destacar que los datos obtenidos son, en cierto punto, concordantes con los estudios realizados por Dodge (2019), Temperini (2020) y De Paoli (2020) sobre las dificultades generales a las que se enfrentan los operadores de

la justicia y la policía en la investigación de este delito. Así, de las entrevistas realizadas se desprende que las principales dificultades del sistema penal de CABA a la hora de investigar estos hechos son: i) el gran aumento de denuncias advertido desde el año 2020 en adelante, toda vez que la cantidad de casos que ingresan a conocimiento del sistema no permite dar una respuesta penal adecuada a todos ellos; ii) la significativa cifra negra. Todos los entrevistados refirieron que el sistema penal toma conocimiento de una pequeña parte de la cantidad de estafas informáticas que se comenten. Además, los bancos no denuncian los casos que advierten o los reclamos que reciben; iii) la falta de capacitación del personal, principalmente de los tribunales. Si bien este estudio puso de manifiesto que las fiscalías especializadas en la materia, el personal del CIJ y el personal policial especializado cuentan con capacitación para investigar ciberfraudes, lo cierto es que eso no sucede con el personal del juzgado, cuyos conocimientos dependen de la voluntad de los propios operadores; iv) la falta de coordinación entre las distintas jurisdicciones del país y la ausencia de protocolos y compromiso por parte de las entidades bancarias, quienes demoran en brindar la información necesaria para investigar y la mutación constante de las maniobras utilizadas por los ciberdelincuentes para cometer estafas *online*.

El segundo de los objetivos específicos pretendía identificar si el sistema penal cuenta con herramientas que incrementen la probabilidad de detección de estafas informáticas y la eventual sanción de los autores. Según esta investigación, el sistema penal tiene diversas herramientas tecnológicas (generadas y adquiridas por el MPF), recursos económicos y humanos para llevar a cabo investigaciones orientadas a detectar delitos de estafa informática. Sin embargo, los participantes de este estudio informaron que la mayor dificultad radica en la propia naturaleza de la web, ya que las pesquisas se complejizan significativamente cuando el dinero se transfiere a billeteras virtuales, circunstancia que dificulta la persecución de los ciberdelincuentes y, en razón de ello, la obtención de sentencias condenatorias.

A raíz de lo expuesto, sería ventajoso dirigir los recursos hacia la creación de herramientas tecnológicas y sistemas de integración de datos entre jurisdicciones que faciliten la realización de investigaciones en aquellos casos en los que el dinero sale del ámbito que - actualmente- alcanza el sistema penal de CABA, así como también profundizar de manera obligatoria la capacitación de los actores intervinientes, incluso la de quienes no integran las unidades especializadas, tal como sugieren Bossler et al. (2019). Por otro lado, los resultados obtenidos en este estudio destacan el problema de la cifra negra y la falta de cooperación de los agentes externos. Es por ese motivo que deberían pensarse alternativas tendientes a reducir estas

dificultades, como por ejemplo la creación de una entidad que unifique los datos de casos de fraude informático y gestione una base de datos que permita reducir los casos provocados por este delito y eche luz sobre los hechos no reportados, como ya lo hace Cifas[22] en Reino Unido, CACF[23] en Canadá o Scamwatch[24] en Australia, quienes además fomentan la cooperación entre el sector público y el sector privado. Además, se debe considerar el establecimiento de protocolos de actuación para los actores externos, similares a los ya implementados en la Estrategia Cibernética Nacional del Reino Unido[25], ya que desempeñan un papel fundamental en las investigaciones. De este modo, será más fácil supervisar las tendencias de estafas informáticas y tomar medidas penales cuando corresponda.

Respecto del tercer objetivo específico, cabe recordar que, desde la perspectiva criminológica, la certeza de ser aprehendido es la variable que más previene delitos en relación con el efecto disuasorio del análisis costo/beneficio del delito (Bottoms & Von Hirsch, 2010; Nagin, 2013; Holt et al., 2017; Maimon, 2020). En línea con ello, los resultados obtenidos en este estudio demuestran que la capacidad del sistema de CABA para actuar de conformidad con esta variable es, a todas luces, escasa: son pocos los casos que llegan a la órbita del sistema penal (cifra negra), son pocas las condenas registradas, ninguna de esas condenas se impuso con prisión de efectivo cumplimiento, en limitadas causas la fiscalía ha logrado recolectar la evidencia necesaria para la realización de un juicio y la mayoría de los casos se han resuelto con salidas alternativas (suspensión del proceso a prueba y reparación integral del daño).

Además, hay casos que quedan sin resolver y, tal como mencionaron los entrevistados, hasta el momento no se ha logrado dar con los responsables de las maniobras denunciadas (quienes finalmente se apropian del dinero), sino que se condena a las "mulas" (eslabones más bajos de la organización criminal). Respecto de la variable celeridad, podría decirse que la investigación de estos delitos no se caracteriza por su rapidez para recabar evidencia. Esto se debe a la complejidad de

[22] Cifas es una organización sin ánimo de lucro dedicada a la prevención del fraude en Reino Unido. Para más información:https://www.cifas.org.uk/about-cifas/what-is-cifas.

[23] El Canadian Anti-Fraud Centre (CAFC) recopila información sobre ciberfraudes. Disponible en: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

[24] Scamwatch tiene como propósito detectar casos de estafa informática y ayudar a su prevención, recopila información sobrehechos por este delito. Ver: https://www.scamwatch.gov.au/about-scamwatch/scamwatch-role.

[25] Se pueden revisar los planes de Estrategia Cibernética Nacional de Reino Unido en https://www.gov.uk/government/cyber-security

la de investigación (tal como sugieren Yar & Steinmetz, 2019; Maimon, 2020; Whelan & Harkin, 2021, entre otros), pero también -y principalmente- a la colaboración de los agentes externos, quienes demoran en la respuesta de la información necesaria para la pesquisa. Respecto de la gravedad del castigo, la sanción fijada para este delito -según los resultados de esta investigación- es suficientemente severa y se ajusta al resto de los castigos previstos en el CP. Sin perjuicio de ello, resultaría conveniente modificar la redacción del artículo 173 del CP a fin de que resulte más fácil identificar los elementos del tipo penal y se puedan perseguir todas las maniobras realizadas por los ciberdelincuentes para estafar, como en el caso del Código Penal Español[26].

En relación con el objetivo general de este trabajo, desde la óptica de la Escuela Clásica y el efecto disuasorio, es posible concluir que la capacidad del sistema penal de CABA para prevenir estafas informáticas es muy limitada. La pena prevista para este delito puede considerarse severa (entre 1 mes y 6 años de prisión), sin embargo, la decisión final sobre la duración de la condena recae en el juez, quien tiene la facultad de ejercer cierta discrecionalidad al imponerla. Además, no existe certidumbre de castigo y la celeridad para arribar a un resultado condenatorio es insuficiente. Esta investigación demuestra que existen significativas ventajas al cometer estafas informáticas como los inmediatos beneficios económicos y que los costos jurídico-penales a los que se enfrentan los ciberdelincuentes son considerablemente menores o, incluso, nulos. Esta disparidad en la relación entre beneficios y consecuencias legales crea, entonces, muy poco desincentivo. El ciberespacio implica un desafío para el sistema penal de CABA y, por lo tanto, es necesario fortalecerlo mediante la implementación de nuevas herramientas y alternativas con el objetivo de aumentar el riesgo de detección de ciberestafas.

Finalmente, este estudio presenta algunas limitaciones, entre ellas, el hecho de que la muestra utilizada ha sido seleccionada de forma deliberada y no representa en su totalidad a los actores intervinientes en la persecución de ciberfraudes. En futuras investigaciones se espera extender la exploración a una muestra de mayor tamaño y

[26] Artículo 249.1. del Código Penal Español: *"También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro."* (lo subrayado me pertenece).

a una mayor diversidad de participantes. Se recomienda, además, realizar una nueva exploración sobre la cifra negra del ciberfraude en CABA, de modo que se logre dimensionar este fenómeno y sus consecuencias, así como también evaluar posibles políticas criminales y de prevención.

VII.- Referencias bibliográficas

- Arimatéia da Cruz, J., & Godbee, N. (2020). Cybercrime Initiatives South of the Border: A Complicated Endeavor. En Holt, T. J., & Bossler, A. M. (2020). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Londres: Palgrave Macmillan.
- Balcarce, F., & Arocena, G. A. (2020). Lecciones de derecho penal: parte especial. Lerner.
- Beccaria, C. (1968). Tratado de los delitos y de las penas. Madrid: Alianza Editorial.
- Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2019). Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. Security Journal, 33(2), 311-328. https://doi.org/10.1057/s41284-019-00187-5.
- Bottoms, A., & Von Hirsch, A. (2010). The Crime-preventive Impact of Penal Sanctions. En Oxford University Press eBooks. https://doi.org/10.1093/oxfordhb/9780199542475.013.0005.
- Cámara Arroyo, S. (2020), "Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente", Revista Derecho y Cambio Social (https://dialnet.unirioja.es/servlet/articulo?codigo=7524987).
- Castro-Toledo, F. J. (2021). Explorando los límites de la disuasión: Un meta-análisis doble sobre la influencia del castigo en el cumplimiento de las normas de propiedad intelectual en Internet. Indret, 2, 1–22.
- Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2021). Police Cybercrime Training: Perceptions, Pedagogy, and Policy. Policing: A Journal of Policy and Practice, 15(1), 15-33. https://doi.org/10.1093/police/pay078.
- Crespo, E. D. (1999). Prevención general e individualización judicial de la pena (Vol. 79). Universidad de Salamanca.
- De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. Policing: A Journal of Policy and Practice, 15(2), 1429-1445. https://doi.org/10.1093/police/paaa027

- Delitos ingresados a las fiscalías y juzgados del Fuero Contravencional, Penal y de Faltas de la Ciudad de Buenos Aires por título y artículo del Código Penal y distribución porcentual por artículo. Ciudad de Buenos Aires. Años 2011/ 2021 | Estadística y Censos. (s. f.). https://www.estadisticaciudad.gob.ar/eyc/?p=75692
- Dodge, C. & Burruss, G. (2019) Policing cybercrime: Responding to the growing problem and considering future solutions. En Leukfeldt, E. R., & Holt, T. J. The Human Factor of Cybercrime. Taylor & Francis.
- Durlauf, S. N., & Nagin, D. S. (2011). Overview of "Imprisonment and crime: Can both be reduced?" Criminology and public policy, 10(1), 9-12. https://doi.org/10.1111/j.1745- 9133.2010.00681.x
- Fuentes, S. C. (2004). La inevitable «mano dura»: sociedad civil y violencia policial en Argentina y Chile. Revista de ciencia política, 24(2). https://doi.org/10.4067/s0718- 090x2004000200001
- Garat, S. & Reale, J. (2018). La reforma penal en materia de cibercrimen en la República Argentina. En Dupuy, D., Llinares, F. M., & Kiefer, M. Cibercrimen II: nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Alianza Editorial.
- Gutiérrez, R. L. (2021). Capítulo 4. Entrevistas estructuradas, semi-estructuradas y libres. Análisis de contenido. En Manuel, T. G. J. (2023). Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario: 171 (ESTUDIOS). Ediciones de la Universidad de Castilla-La Mancha.
- Gómez-Bellvís, A. B., Piquero, A. R., Miró-Llinares, F., Piquero, N. L., & Castro-Toledo,
- F. J. (2023). Certainty, But How Certain? Severity, But How Severe? A Quasi- Experimental Study on Digital Piracy Deterrence in a Spanish Citizens Sample. Crime & Delinquency, 001112872311701. https://doi.org/10.1177/00111287231170110
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). Cybercrime and digital forensics: An introduction. Retrieved from http://ebookcentral.proquest.com
- Jewkes, Y., & Yar, M. (2010). Introduction: the Internet, cybercrime, and the challenges of the 21st century. En Y. Jewkes & M. Yar (Eds.), Handbook of Internet crime. Willan Publishing.
- Kemp, S., & Moneva, A. (2020). Fraude online vs. offline: factores predictores de victimización y su impacto. Indret: Revista para el Análisis del Derecho, 1, 15. https://dialnet.unirioja.es/servlet/articulo?codigo=7266745

- Kemp, S., Miró Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. European Journal on Criminal Policy and Research, 26(3), 293-312. https://doi.org/10.1007/s10610-020-09439-2
- Larrauri Pijoan, E. (1998). Criminología crítica: abolicionismo y garantismo. Ius Et Praxis, 4(2). http://www.cienciaspenales.net/descargas/idp_docs/doctrinas/elenalarrauri.pdf
- Larrauri Pijoan, E. & Cid Moline, J. C. (2001). Teorías criminológicas: Explicación y prevención de la delincuencia. Barcelona: Editorial Bosch S.A.
- Larrauri Pijoan, E. (2018) Introducción a la criminología y al sistema penal. Segunda edición revisada. Madrid: Editorial Trotta.
- Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. L. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. Crime Law and Social Change, 67(1), 77-96. https://doi.org/10.1007/s10611-016-9648-0
- Linares, M. B. (2021). Delitos informáticos en el Código penal argentino. Revista Chilena de Derecho y Ciencia Política, 11(2), 122-144. https://doi.org/10.7770/rchdcp-v11n2- art2289
- Maimon D. (2020). Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature. En Holt T., Bossler A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_24
- Maras, M. H. (2022). Compendio de ciberdelincuencia organizada. Revista Pensamiento Penal.
- Martí, J. (2018). Diseños de investigación social y métodos. Centre d'Estudis Sociològics Sobre La Vida Quotidiana i El Treball Institut d'Estudis Del Treball Departament de Sociologia. Universitat Autònoma de Barcelona.
- Martínez, M. S. (2017). Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil. En Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet. Compilado por Ricardo Antonio Parada; José Daniel Errecaborde. (1.a ed.). Erreius.
- Maxfield, M. G., & Babbie, E. R. (2014). Research Methods for Criminal Justice and Criminology. Cengage Learning.
- Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista electrónica de ciencia penal y criminología, 13, 7. http://criminet.ugr.es/recpc/13/recpc13-07.pdf

- Miró Llinares, F. (2012). El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons.
- Miró Llinares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. Revista Electrónica de Ciencia Penal y Criminología, vol. 15.
- Miró Llinares, F., & Gómez Bellvis, A. B. (2018). La estafa informática: fenomenología y respuesta jurídica. En Dupuy, D., Llinares, F. M., & Kiefer, M. Cibercrimen II: nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Alianza Editorial.
- Miró Llinares, F., & Gómez Bellvís, A. B. (2022). La Estafa Informática: Fenomenología y Respuesta Jurídica. En Cibercrimen II (2.a ed.). B de F.
- Miró Llinares, F., & Ortuño, R. B. (2013). ¿Por qué cumplimos las normas penales? Sobre la disuasión en materia de seguridad vial. InDret, 4, 18-53. http://www.indret.com/pdf/1001.pdf
- Ministerio del Interior, Secretaría de Estado de Seguridad. (2021). Informe sobre la cibercriminalidad en España. Gobierno de España.
- Nagin, D. S. (2013). Deterrence in the Twenty-First Century. Crime and Justice, 42(1), 199-263. https://doi.org/10.1086/670398
- Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An Exploration of the Psychological Impact of Hacking Victimization. SAGE Open, 11(4), 215824402110615. https://doi.org/10.1177/21582440211061556
- Raggio, S & Cipriano García, R. (2023). Las consecuencias sociales de la mano dura en la Argentina. CLACSO - Consejo Latinoamericano de Ciencias Sociales | Conselho Latino-americano de Ciências Sociais. https://www.clacso.org/las-consecuencias- sociales-de-la-mano-dura-en-la-argentina/.
- Roxin, C. (1997). Derecho Penal. Parte General. Madrid: Editorial Civitas.
- Simaz, A. L. (2020). Manual de derecho penal: parte especial. Erreius.
- Sosa, M. E. (2023). Evidencia digital: Su importancia en la investigación. Revista Pensamiento Penal. https://www.pensamientopenal.com.ar/doctrina/90772-evidencia-digital-su-importancia-investigacion
- Temperini, M. (2018). Delitos informáticos y cibercrimen: técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales. En Dupuy, D., Llinares, F. M., & Kiefer, M. Cibercrimen II: nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal.

Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Alianza Editorial.

- Temperini, M. (2015). El desafío de la lucha contra el cibercrimen en Argentina. Papeles del Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales, 16, 31-51. https://doi.org/10.14409/p.v0i16.4832.
- Whelan, C., & Harkin, D. (2021). Civilianising specialist units: Reflections on the policing of cyber-crime. Criminology & Criminal Justice, 21(4), 529-546. https://doi.org/10.1177/1748895819874866
- Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications Limited.