Título: Criptoactivos y los desafíos pendientes. Modelos de datos alternativos aplicados al criminalidad económica con uso de criptoactivos

Autores:

Germán Silva. Antropólogo, docente de postgrado de la Universidad de Buenos Aires (UBA) y de grado en la Universidad Nacional de Quilmes (UNQ), autor de publicaciones relacionadas a las metodologías de investigación, específicamente del "*social network analysis*" y su aplicación en el ámbito penal. Se ha desempeñado en el Ministerio Público Fiscal y actualmente la Corte Suprema de Justicia de la Nación.

Marina Marsili. Contadora Pública especializada en Administraciòn y Contabilidad Pública, Doctora en economía (UNR). Abogada (Universidad Siglo XXI). Subsecretaria administrativa del MPF. Docente universitaria.

Resumen

La creciente adopción de criptomonedas ha generado nuevas oportunidades para actividades ilícitas, tales como el lavado de dinero, el financiamiento del terrorismo y el fraude. La naturaleza descentralizada y pseudoanónima de los criptoactivos dificulta la detección y prevención de estos crímenes mediante métodos tradicionales.
Por ello, se propone la aplicación de la metodología *Social Network Analysis* (SNA - ARS en su siglas en español), sumado a las nuevas posibilidades de las nuevas inteligencias artificiales, como herramientas claves para identificar patrones de comportamientos y relaciones entre actores involucrados en actividades criminales con criptoactivos. El SNA permite relevar, mapear y analizar las redes de interacción, destacando nodos/personas y vinculaciones críticas que pueden ser indicativos de actividades ilícitas.

El presente trabajo surge del trabajo conjunto de los integrantes del proyecto académico titulado "Criptactivos. Herramientas contables y jurídicas para la prevención e investigación de delitos cometidos a través de operaciones con activos digitales", en el marco del *Programa de Estudios Interdisciplinarios sobre Prevención y Persecución de la Criminalidad Económica del Centro de Estudios Interdisciplinarios de la Universidad Nacional de Rosario.*

I. Introducción

El hecho de que la revolución digital haya transformando el sector financiero tradicional, creando nuevas prioridades y oportunidades, en su total abanico de posibilidades de uso: tanto aquellas alineadas con la legislación de cada Estado, aquellas que se bifurcan levemente, y finalmente aquellas que se encuentran al margen de lo establecido por la normativa penal.

Por lo cual en el presente artículo hemos de entender que dichas nuevos espacios también han provocado un terreno fértil para materializar hechos ilícitos y canalizar fondos derivados de la economía criminal, esquivando así los controles públicos.

El uso de monedas virtuales, debido a su naturaleza anónima y dinamica, casi como una verdad de perogrullo, pareciera facilita la perpetración de ilícitos, tales como el lavado de dinero, el financiamiento del terrorismo y el fraude. La naturaleza descentralizada y pseudoanónima de los criptoactivos, *a priori*, dificulta la detección y prevención de estos hechos sociales criminales mediante métodos tradicionales.

En este contexto, las redes criminales, al igual que todas las redes que constituimos los humanos en los hechos sociales, se encuentran en constante adaptación. Probablemente algunas redes criminales se adapten mejor que otras a los nuevos entornos, siendo aquellas que logren utilizar de manera más eficiente los recursos que a su disposición se encuentran. En este artículo nos centraremos en los recursos derivados de la revolución en las tecnologías financieras.

La adaptación a que hacemos referencia se funda en dos ejes: el primero de ellos refiere al conocimiento necesario para la utilización de dichas tecnologías, mientras que el segundo eje se erige sobre cómo utilizar dichas tecnologías para evitar el control de los Estados. Este segundo será central, pues es la variable que distingue entre los obstáculos derivados de toda revolución tecnológica a la que se someten los individuos, y aquellos obstáculos propios de las redes que nos ocupan, las empresas criminales.

Este escenario, por otro lado, exige al Estado un nivel de especialización y formación en los investigadores igual o superior al de las redes criminales. Además, requiere la disponibilidad de herramientas digitales específicas y, sobre todo, la implementación de un enfoque interdisciplinario en las agencias de regulación, investigación y control. Es fundamental destacar la importancia de este enfoque interdisciplinario, ya que al enfrentarse a redes de criminalidad compleja, que son altamente interdisciplinarias, la complejidad criminal se beneficia de esta integración de conocimientos. En contraste, los organismos estatales a menudo operan bajo una ilusión de trabajo conjunto entre disciplinas que, en realidad, no alcanzan la misma profundidad de las redes contra las que luchan.

Frente a estos desafíos, el objetivo es llevar a cabo una investigación que nos permita identificar las fortalezas y debilidades estatales respecto a la prevención y persecución de delitos cometidos con criptoactivos para diseñar mecanismos de control y prevención; y analizar herramientas de investigación disponibles, como así también aproximaciones teóricas.

II. Tipos de delitos vinculados a criptoactivos

Las criptomonedas, debido a su naturaleza digital y descentralizada, han surgido como una nueva frontera tanto para la innovación financiera como para la actividad criminal. Como yo lo hemos dicho, este panorama introduce nuevos métodos en la materialización de los ilícitos, que frente a aquellos que pueden considerarse como "*tradicionales*" requieren otro grado de especialización y formación de los investigadores, la disponibilidad de herramientas digitales específicas y una adecuada interdisciplina, principalmente entre los profesionales de las ciencias económicas, los profesionales de las ciencias informáticas, y de todas aquellas disciplinas que se han especializado en la investigación social desde hace más de un siglo.

Las redes criminales están en continuo cambio, buscando obtener día a día nuevos mecanismos para sortear los controles que ejercen los distintos organismos. En este sentido, el nuevo mercado que plantea el uso de activos virtuales pareciera convertirse en un nueva arena social ideal para cometer ilícitos. A medida que su popularidad y adopción aumentan, también lo hacen las formas en que pueden ser explotadas para actividades ilícitas.

Todo delito complejo conlleva la coexistencia de distintos tipos de delitos que se suceden en forma paralela o intermitente y en diferentes magnitudes, y una de sus principales características es la mutabilidad. Para dar cuenta de dicha características, a continuación se listan los tipo de delitos asociados con criptoactivos, destacando en cada caso, las técnicas utilizadas para dificultar la investigación y el rastreo de estos fondos.

A continuación, a partir de una prospección sucinta de noticias periodísticas se identifican algunas de las prácticas más comunes. La primera descripta -*Initial Coin Offerings*- ha afectado significativamente al mercado de las criptomonedas generando una desconfianza en un gran sector de la sociedad, pues son las que más se han divulgado en los medios de comunicación. Pero no son los únicos modos registrados de utilización de criptoactivos, es por ello que se presentan un abanico de posibilidades de utilización del ecosistema de las nuevas tecnologías financieras vinculadas a tipos de delitos, con sus respectivos ejemplos en algunos casos, por si los lectores desean profundizar en algún tipo en especial.

Generalmente bajo el desarrollo de falsos proyectos, o basados en equipos inexistentes, y/o promesas exageradas sobre las supuestas ganancias. También se registran modos criminales de mayor vinculación a los modos tradicionales, como la suplantación de identidad (a través de phishing informático, o simples hackeos de contraseñas).

- Fraude en las ICO (*Initial Coin Offerings*)**:** El fraude en ofertas iniciales de monedas implica la venta fraudulenta de tokens. Este tipo de fraude puede incluir falsedades sobre la empresa detrás de la ICO, publicidad engañosa y otras tácticas para estafar a los inversores.
    - Caso Giza: Los fundadores de esta ICO no lograron ser contactados tras recaudar más de $2 millones. Los inversores nunca recibieron sus tokens, y se cree que la ICO fue una estafa.
    - Rivetz: En 2018, la Comisión Nacional de Valores (CNV) de Argentina advirtió sobre una empresa que ofrecía inversiones en la criptomoneda "Rivetz". La empresa fue denunciada por estafa y el CEO fue detenido.

- Estafas de Inversión: Las estafas de inversión en criptomonedas pueden presentarse de diversas formas, generalmente involucrando promesas falsas de altos rendimientos y retornos rápidos.
    - BitConnect: Acusada de ser un esquema Ponzi, dicha plataforma de préstamos llevó a los inversores a perder millones de dólares. El fundador fue arrestado.
    - Proyecto Wallet: En 2019, la policía argentina arrestó a un hombre acusado de estafar a cientos de personas mediante esta plataforma de inversión, con pérdidas estimadas en 15 millones de dólares.

- Robo**:** implica acceder ilegalmente a una billetera digital o cuenta de intercambio (*exchanges*) para sustraer monedas.
    - Coincheck, Japon: En 2018, esta plataforma de intercambio fue hackeada, resultando en el robo de más de $500 millones en NEM (moneda virtual no tan conocida, pero de gran capitalización en mercado).
    - Ciudad del Este, Paraguay: Un grupo de delincuentes robó más de 2 millones de dólares en criptomonedas de una empresa de minería en 2018, utilizando armas de fuego para perpetrar el robo.

- Extorsión: ocurre cuando un atacante exige un rescate en criptomonedas a cambio de no divulgar información privada o comprometedora.
    - WannaCry: ransomware que exigía pagos en Bitcoin para desbloquear sistemas infectados. El ataque afectó a más de 200.000 computadoras y los hackers obtuvieron alrededor de $140.000 en Bitcoin.
    - México: un grupo de hackers que extorsionaba a empresas exigiendo pagos en criptomonedas fue descubierto en el año 2020.

- Intermediación financiera no autorizada: cuando por cuenta propia o ajena, directa o indirectamente, se realizan actividades de compra, venta, ofrecimiento, colocación de valores negociables u otros instrumentos financieros como cheques, pagarés, acciones, letras de cambio, sin la debida autorización del Banco Central de la República Argentina o la Comisión Nacional de Valores. Por tanto, consiste en la posibilidad de procurar y conseguir recursos financieros del público para luego prestarlos al público, con lo cual deben darse los dos aspectos de la actividad regulada: la oferta y la demanda: se toman depósitos a plazo y se colocan estos fondos, el intermediario financiero se fondea en su actividad de prestar sobre lo que previamente tomó a plazo. (Greppi, 2022)

  La norma tiene como objeto los recursos financieros (art. 1 de la ley n° 21.256), entendidos como el dinero y otros activos financieros que por su liquidez puedan cumplir una función similar. Este elemento y las características propias de los criptoactivos lo hacen objeto de maniobras que se encuentran reguladas por la normativa en tanto las criptomonedas como recursos financieros que podrían ser objeto de la conducta punible de intermediación que define el art. 310. párr. 1° del C.P.

- Lavado de Dinero (De la Cruz Pinto, 2015; Marsili, 2019, Marsili, 2020): La sanción de la Ley 26.683 en 2011 marcó un hito significativo en la lucha contra este delito en Argentina, al reconocerlo como un delito autónomo. Ello reconocimiento no solo reflejó una evolución normativa, sino que también subrayó la naturaleza pluriofensiva del lavado de activos, destacando sus múltiples y graves consecuencias a nivel económico, social e institucional.

  El lavado de dinero con criptoactivos implica ocultar el origen ilegal de los fondos mediante transacciones financieras. Al igual que ocurre con el resto de los activos utilizados en el lavado de dinero, se parte de la premisa que todo ilícito que genere beneficios económicos conlleva luego operaciones más o menos eficaces de disimular su origen. A este escenario se enfrentan los agentes involucrados en la investigación o persecución penal que deben identificar las acciones desplegadas como maniobras destinadas a alterar la percepción respecto del origen de los activos en poder de la organización criminal. El lavado de activos implica la inserción de bienes o dinero de origen ilícito en la economía, afectando el funcionamiento normal de todos los sectores, incluidos el financiero, productivo y familiar. La principal función de esta maniobra es ocultar o enmascarar el verdadero origen de estos activos, permitiendo que la economía social los absorba.

Profundizando más en este uso de criptoactivos, desde una mirada criminológica, el lavado de activos permite que las organizaciones criminales se consoliden económicamente, robustezcan sus estructuras, potencien su accionar criminal y disfruten con mayor facilidad de los activos espuriamente obtenidos. Esto, a su vez, facilita la

comisión de nuevos delitos y perpetúa un ciclo de actividad criminal (Marsili, 2020). Este proceso no solo facilita la comisión de nuevos negocios ilícitos, sino que también aumenta los beneficios de las organizaciones criminales, profundizando el daño a la calidad de vida de los habitantes y afectando variables económicas clave como el producto bruto interno geográfico, el consumo familiar, los precios y la recaudación fiscal.

Como se ha observado en la enumeración de tipos y modos de utilización de los ecosistemas virtuales, existe una gran variedad de conductas y formas de relacionamiento entre los diferentes agentes involucrados. Esta diversidad puede llevar inicialmente a la percepción de un aumento en la complejidad. Sin embargo, una pregunta que deberíamos plantearnos pronto es si las estructuras reticulares profundas que se establecen entre las personas en los distintos modos son, en realidad, semejantes. Esto nos permitiría categorizar los fenómenos en función de una o unas pocas topologías que emergen de los vínculos sociales.

III. Maniobras comunes para evitar el rastreo o dificultar la investigación

Es inevitable destacar que al contrario de lo que a primera vista se suele pensar, intuitivamente, que la ya reiterada característica de pseudoanonimato es el principal valor que posee estas nuevas tecnologías para su uso en actividades ilegales. Lo cierto es que el uso de empresas "*exchanges*" han incrementado su relevancia en dicho mercado. La curva de aprendizaje en la adopción de dichas nuevas tecnologías, tanto para el sectores legales como ilegales, ha supuesto el surgimiento de un nuevo rol que día tras día aumenta su *centralidad de intermediación* en las redes de transacciones de criptoactivos.

Por lo cual en términos globales, el anonimato característico de dichos activos pareciera ir diluyéndose a medida que dichos agentes han irrumpido con fuerza en el mercado. Esto se explica por el simple motivo que para operar en dichas *exchanges* hay que registrarse, o al menos poseer modos de autentificación para poder operar, y con ello rompen con el ya famoso anonimato. Por lo cual, a partir de dicho momento, toda transacción pareciera quedar condenada idealmente a la perfecta trazabilidad de fondos.

A partir del surgimiento de dichas plataformas, los usos legales e ilegales parecieran o deberían comenzar a bifurcar sus caminos evolutivos. Ninguna organización criminal, *a priori*, vería alguna ventaja en su capacidad operativa en transacciones fácilmente rastreables, algo que el dinero fiduciario permite con mucha mejor performance. Por lo cual, para abocarnos a la utilización de criptoactivos en el contexto de actividades ilícitas, deberíamos alejarnos en una primera instancia del uso de las plataformas *exchanges*.

A continuación se presentan algunos de las técnicas utilizadas por las organizaciones criminales para dificulta el rastreo de sus operaciones:

- *Peeling Chain*: Es la técnica utilizada para lavar grandes cantidades de criptomonedas obtenidas ilegalmente mediante la financiación de una larga serie de pequeñas transacciones. Pequeñas cantidades se "pelan" de las tenencias de una persona en transferencias de bajo valor repetidas veces, a menudo a través de un intercambio donde se pueden convertir a moneda fiduciaria.

- *Cross-Chain Swap*s: Los cross-chain swaps o intercambios atómicos entre cadenas permiten a los usuarios intercambiar directamente criptomonedas entre distintas blockchains sin intermediarios -recordemos cada moneda posee su propio registro denominado blockchain-. Aunque no son ilegales y son ampliamente

utilizados, a veces pueden ser usados para ocultar el movimiento de fondos. Estos intercambios mejoran la interoperabilidad entre blockchains y facilitan el acceso a una variedad de criptomonedas.

- Los *Mixers* (mezcladoras) son servicios diseñados para aumentar la privacidad de las transacciones que permiten mezclar transacciones para dificultar su rastreo. Funcionan mezclando las criptomonedas de varios usuarios para "disfrazar" su origen, de modo que sea difícil rastrear de dónde provienen y a dónde se dirigen los fondos. Servicio ideal para quienes estén interesados en dificultar la capacidad de reconstruir la trazabilidad de los fondos. Cabe mencionar sobre este último punto, que en Argentina, se ha detectado el uso de *mixers* en el caso del *Virus Mekotio*.

IV. El mercado y la economía criminal

Las organizaciones delictivas utilizan innovaciones en producción, distribución y consumo de bienes y servicios, aprovechándose de las debilidades del Estado en materia de controles y regulación. Estas organizaciones establecen estructuras sólidas, diversificando sus actividades entre negocios legales e ilegales, y se interrelacionan con actores de diferentes orígenes y pertenencias.

La investigación –por tanto- debe considerar estas innovaciones y adaptarse a ellas para comprender mejor el funcionamiento de las organizaciones criminales, incorporando otras metodologías de investigación provenientes de ciencias no jurídicas para dotar de mayor profundidad al análisis de la información.

Es importante no obstante, tener presente que el mercado es el ámbito donde se desarrollan intercambios de bienes o servicios entre individuos. Por ello, una investigación penal exitosa requerirá interpretar las formas de vinculación de los actores, las herramientas que utilizan, los roles en la organización, canales de comunicación, actividades legales e ilegales, y vínculos internos y externos. También será esencial estudiar el mercado en que opera la organización, identificando precios, estructuras de negocios, volúmenes, mecanismos de pago, legislación, regímenes sindicales y formas de comercialización.

Obtener información respecto de la organización criminal y de los delitos cometidos por esta, serán tareas primordiales que deberá desplegarse a la vez que se procuren detectar los activos de la organización criminal para adoptar medidas cautelares oportunas y establecer acciones de decomiso; identificar al beneficiario final de los activos y quienes aparecen como titulares registrales, y comprender las relaciones entre los sujetos y el funcionamiento de la organización.

IV.a Obtención de información y análisis

Investigar el crimen organizado es una tarea compleja y desafiante debido a una serie de factores, entre ellas cabe referir que las organizaciones criminales operan en secreto y mantienen una estructura clandestina para ocultar sus actividades, muchas de ellas lo hacen a nivel transnacional, lo que demanda nuevas formas de lograr el flujo tanto de mercaderías como de dinero, lo que hace que se encuentren en continua modificación, adoptando nuevas tecnologías entre las que se pueden enumerar el uso de

criptomonedas, la *dark web* y el cifrado de comunicaciones. Estas herramientas, a raíz de su naturaleza anónima, dificultan el seguimiento de sus actividades y el rastreo de las transacciones.

Estas complejidades son las que se enfrentan las diferentes agencias a diario y que hacen que la investigación del crimen organizado sea un proceso complejo y de largo plazo que requiere la cooperación y coordinación entre diferentes organizaciones, así como el uso de tecnologías y estrategias innovadoras.

Para obtener información primaria de calidad, se deben identificar las personas implicadas, conocer su entorno, relevar los bienes identificados y verificar su titularidad; analizar operaciones registradas como resúmenes de cuentas bancarias, formas de pago, transacciones en casas de cambio, giros de dinero, transferencias bancarias, compra de divisas, participación en sociedades, y actividades económicas sospechosas.

Los criptoactivos adicionan un nuevo activo a analizar que incorpora una dificultad técnica que invita a explorar.

IV.b Contexto y desafíos

Los desafíos en el abordaje de los aspectos económicos de los delitos son fundamentales para atacar las estructuras delictivas complejas que afectan tanto al sistema económico como al social. Es crucial conocer la organización criminal para proyectar investigaciones financieras efectivas. Las empresas criminales tienen vida propia y su análisis debe partir de las actuaciones vinculadas a la causa judicial y la estrategia de investigación, considerando los delitos investigados, el contexto, los sujetos involucrados y otros elementos que permitan analizar la tipicidad objetiva y subjetiva.

Los elementos que componen una organización criminal son inciertos y cambiantes, siguiendo los postulados de Etkin son complejos (2006). La investigación de delitos complejos representa uno de los mayores desafíos para el sistema de justicia. La coexistencia de subtipos de delitos que operan en paralelo o intermitentemente, y en diversas magnitudes, requiere un enfoque integral que aborde no solo el hecho principal sino también las ramificaciones económicas y organizativas que lo sostienen. Este documento explora las técnicas, herramientas y metodologías necesarias para una efectiva investigación de organizaciones criminales complejas.

Epistemologia de una producción de información estratégica

La producción de información estratégica es esencial en la investigación de delitos complejos. Según Morin (2009), el conocimiento se genera a partir de la selección de datos significativos y la exclusión de los irrelevantes. Este proceso implica la clasificación, jerarquización y centralización de datos que se transforman en información cargada de significado, con un objetivo concreto y efectos determinados.

La utilización de tecnologías avanzadas y la inteligencia artificial pueden facilitar la transformación de datos en información estratégica, mejorando la eficiencia de las investigaciones. Davenport y Prusak (1998) destacan la importancia de identificar, estructurar y utilizar la capacidad analítica para interpretar estos insumos, determinando qué tipo de información y conocimiento son necesarios para la investigación.

Para ello, la metodología en la investigación criminal debe incorporar elementos de planificación y evaluación, atendiendo a la política criminal definida. La planificación permite establecer metas realistas y concretas, desarrollar hipótesis de trabajo y estrategias específicas. Esto facilita el control de las acciones, el registro histórico del caso, y la optimización de los recursos disponibles.

La estructura de los equipos de investigación es fundamental. Estos deben ser pequeños, altamente capacitados, profesionalizados e interdisciplinarios, incluyendo expertos en áreas como economía, ciencias sociales e informática. La proactividad y una comunicación horizontal dentro de los equipos son cruciales para abordar los delitos complejos, que no se pueden circunscribir a un solo hecho.

Innovación en la estructura de investigación

La investigación de delitos complejos requiere de estructuras innovadoras y flexibles, capaces de adaptarse a las modificaciones del contexto. La dirección de estas investigaciones debe ser creativa, innovadora en métodos y formas de abordaje, y capaz de operar en un entorno de "caos creativo". Los equipos deben estar abiertos al pensamiento lateral y a nuevas formas de investigación y recolección de datos.

La magnitud de datos relevados en la investigación de delitos complejos exige una adecuada clasificación, etiquetado e inserción en bases de datos. Esto permite un posterior procesamiento y análisis conforme al tipo de investigación, el delito perseguido y el plazo temporal asignado. La recopilación de información debe pasar por las etapas de compilación, limpieza, almacenamiento y categorización, con un filtrado eficaz para garantizar la calidad de los datos.

La idea de que la política criminal debe ser una labor estratégica ha sido utilizada por diversos autores, incluido Binder, para enfatizar el contraste con las lógicas burocráticas que tradicionalmente han determinado las lógicas de selectividad de la política criminal (Binder, 2013).

Los caracteres esenciales de lo que ha sido denominado como política criminal estratégica son:

i. Planificación: que tenga el qué, cómo, cuándo, dónde, con qué. Adaptabilidad y flexibilidad: ajustándose a las cambiantes dinámicas de la delincuencia y la conflictividad.
ii. Evaluación y monitoreo: seguimiento constante y una evaluación rigurosa de las intervenciones y políticas implementadas para ajustar las estrategias según sea necesario y garantizar que las políticas sean efectivas.
iii. Enfoque interdisciplinario y multidimensional: Adoptar un enfoque interdisciplinario que incorpore conocimientos y perspectivas de diversas disciplinas, como economía, sociología, antropología, criminológico, para comprender mejor la complejidad de los delitos económicos y sus vínculos con la regulación estatal.

Se requieren estructuras innovadoras, con mecanismos de interacción con otras áreas de gobierno, y colaboración internacional. Una dirección creativa, que permita un poco de desorden, un poco de flexibilidad, innovadoras en sus métodos, con capacidad de mutar; abierta en la lectura de los mercados donde opera la empresa criminal. Los equipos deben ser proactivos, abandonando la lógica del caso a caso; capaces de considerar los problemas desde nuevos ángulos, pero partiendo de una batería de medidas, a las cuales apelar para comenzar a conocer el problema.

Un grupo de investigación interdisciplinario que se ocupe de relevar la estructura económica en la cual se inserta la organización; conocer el Mercado, precios, estructuras de negocios, volúmenes, mecanismos de pago/cobro, formas de comercialización y distribución, instituciones financieras, mercado de capitales y ahorro, regímenes sindicales.

Equipos capacitados e interdisciplinarios son fundamentales para la investigación de delitos complejos con maniobras que involucran criptoactivos tornan necesario el conocimiento de expertos de otras materias alejadas al derecho penal y resultan necesarios profesionales vinculados a las ciencias económicas, sociales, informáticas, entre otras.

Abordajes alternativos para analizar la información que surja de las distintas etapas del proceso cognitivo con un doble propósito: obtener referencias que contribuyan a diseñar la estrategia de persecución penal, por un lado, e identificar modos de gestión de los recursos materiales y humanos por parte de las organizaciones criminales para reciclarlos en ocasión de proceder a diseño de las tareas de seguridad preventivas, por el otro.

Los flujos y las formas de trabajo requieren proactividad, abandonar la lógica del caso a caso y las “baterías” de sugerencias de medidas. La dirección de estos equipos, más allá de la horizontalidad con la que cuentan y la expertise propia de cada uno, estará en cabeza de la autoridad judicial o exclusivamente fiscal en un futuro, que lleven adelante la investigación los cuales deben ser dinámicos, tener un conocimiento completo del entorno criminal, así como de los instrumentos legales, y por sobre todas las cosas, la capacidad de poder ver más allá del aquí y ahora.

Estos equipos deben ser capaces de considerar los problemas desde nuevos ángulos, tener una base de medidas a las cuales apelar para comenzar a conocer el problema y acomodar sus partes constitutivas, pero sin olvidar que para poder abordar las organizaciones complejas deben estar abiertos al pensamiento lateral, a salir de las formas típicas de investigación y recolección de datos.

Estrategias de investigación, persecución penal y colaboración interinstitucional

El sistema preventivo debe identificar operaciones que pretendan introducir fondos ilícitos en el sistema formal. La prevención requiere la obtención de datos y la producción de información pública para evitar que el producto del delito se integre en la economía formal. La colaboración entre distintas áreas del gobierno, tanto económicas, tributarias, legales como de seguridad, es esencial para generar un clima de cooperación en la lucha contra estos delitos.

Las investigaciones judiciales han demostrado que las economías legales e ilegales se imbrican y entrelazan. Las organizaciones delictivas montan estructuras con apariencia de legalidad mediante la manipulación de figuras societarias y la constitución de empresas transnacionales, lo que facilita la canalización de divisas hacia países centrales (Biscay, 2016).

En otros términos como lo ha detallado Salcedo y Garay (2016), las políticas criminales deberían estar centradas en la identificación de aquellos sujetos que operan en las denominadas zonas grises. La idea de dichos autores se resumen en que los miembros de las organizaciones criminales operan tanto en la ilegalidad plena como en lo que se conoce como "*zonas grises*", es decir, áreas donde sus actividades pueden no ser completamente ilegales, pero aun así pueden ser consideradas de relevancia estratégica para el desmantelamiento de dichos entramados. Por lo cual, trabajar con metodologías de investigación que nos otorguen indicadores cuantitativos sobre los roles que desarrolla cada sujeto en un entramado social investigado es de suma importancia.

Solo mediante un enfoque integral y sostenido se podrá desmantelar económicamente a las bandas criminales y proteger la salud del sistema económico y la confianza de los ciudadanos en las reglas de la economía. Crear fiscalías especializadas concebidas desde la misma lógica de la complejidad, que establezcan mecanismos de trabajo horizontales y flexibles para la sistematización de datos, obtención de información y procesamiento a través de una mirada multidisciplinaria (económico, político y antropológica) pareciera el único camino que debemos recorrer si queremos alterar el desequilibrio de fuerzas entre las redes criminales y las redes estatales que procuran la lucha contra las primeras.

Por lo cual, todo lo dicho sobre las estructuras que cometen delitos complejos ya que cuentan con un alto nivel de dinámica intrínseca, hecho por el cual las organizaciones destinadas a su investigación también deberían poseer las más mismas cualidades:

- *Adaptabilidad*. Los equipos de trabajo deben ser capaces de pensar estrategias innovadoras para el abordaje de delitos complejos, conforme se registran modificaciones del contexto.

- *Coordinación interinstitucional*: La cooperación y coordinación entre las diversas agencias e instituciones involucradas en la prevención del delito y la justicia penal.

- *Sostenibilidad:* Las políticas criminales deben ser diseñadas e implementadas de manera que sean sostenibles en el tiempo, teniendo en cuenta la disponibilidad de recursos y la capacidad de las instituciones para llevar a cabo las intervenciones planificadas.

Identificación de activos y beneficiarios finales

La identificación de activos puede ser vista como una acción orientada al decomiso o como una estrategia compleja asociada a la producción de información, con el objetivo de desarticular las redes que financian actividades criminales.

La identificación de activos es crucial para adoptar medidas cautelares, como el decomiso, que reduzcan la capacidad operativa de las organizaciones criminales. Es necesario identificar tanto a los titulares registrales como a los beneficiarios finales de estos activos, comprendiendo cómo operan las organizaciones y cuáles son sus estructuras de poder.

La proliferación de ciberdelitos como estafas, phishing, compras en mercados ilegales entre otros, subraya la urgente necesidad de poseer recursos tecnológicos y humanos especializados para combatirlos. Sin embargo, las limitaciones presupuestarias de los ministerios públicos para adquirir o formar dichos recursos y capacitarlos de

manera constante plantean la necesidad de explorar nuevas alternativas. Una posible solución es que el propio combate a los ciberdelitos genere los recursos necesarios para ello.

El objetivo es acabar con toda una operatoria criminal, recuperando no solo los fondos robados a la víctima denunciante sino también cualquier ganancia obtenida por la inversión de criptoactivos. Estos fondos adicionales pueden ser destinados a la adquisición y mantenimiento de hardware y software especializado, así como a la capacitación de recursos humanos para combatir los nuevos modos de criminalidad, como lo es todo lo relativo al mundo cripto.

En investigaciones relacionadas con phishing, por ejemplo, se observa que los fondos obtenidos ilícitamente son frecuentemente convertidos en criptoactivos. Esta conversión se realiza con el objetivo de perder la trazabilidad de los activos y, a su vez, lograr la impunidad de los delincuentes. A menudo, los delincuentes realizan transacciones con valores superiores a los robados, lo que sugiere que estos fondos podrían ser de otras víctimas. Para llevar adelante esta estrategia, es necesario trabajar en dos frentes: a) hacia afuera y b) hacia adentro del ministerio público.

- Frente “Hacia fuera”
    a. Campañas de Denuncia: Difundir la importancia de denunciar ciberdelitos a través de campañas publicitarias.
    b. Convenios con entidades financieras: Establecer asociaciones con bancos y entidades financieras para incentivar a sus clientes a denunciar y para que entreguen rápidamente la información requerida por oficio judicial, previo levantamiento del secreto bancario.

- Frente “Hacia dentro”
    a. Protocolos de Actuación: Establecer protocolos claros para la actuación desde el momento de la denuncia y durante el trabajo de los fiscales.b)
    b. Fiscalías Especializadas: Crear fiscalías especializadas en ciberdelitos, las cuales no necesitan ser por ciudad o distrito, sino que pueden ser regionales o provinciales debido a la naturaleza virtual y global de los criptoactivos.

Procedimiento de recupero de activos

El proceso de recuperación de activos involucra varias etapas críticas, cada una con un conjunto específico de acciones destinadas a asegurar la identificación, localización, y recuperación efectiva de los activos involucrados en actividades ilícitas o sospechosas. A continuación, se describe un esquema general del procedimiento basado en estas etapas:

a. Identificación de las Personas Involucradas

Recolección de Datos Personales: Se debe iniciar el proceso obteniendo información básica y necesaria sobre las personas involucradas, tales como nombre, apellido, número de documento, CUIT o CUIL. Esta información es fundamental para realizar las consultas pertinentes ante diferentes organismos.

Levantamiento del Secreto Fiscal, Bancario y Financiero: Es crucial solicitar el levantamiento de los secretos fiscales, bancarios y financieros para obtener acceso a toda

la información relevante que pueda estar protegida por confidencialidad. Este paso permite una visualización completa de las transacciones y activos de las personas investigadas.

Determinación del Periodo de Investigación: Es necesario establecer un periodo de tiempo específico para circunscribir la investigación, lo que permitirá focalizar la búsqueda de activos y transacciones relevantes dentro de un marco temporal determinado.

b. Solicitud de Información a Entidades Relacionadas

Banco Central de la República Argentina (BCRA): informe detallado de la totalidad de cuentas bancarias y cuentas digitales registradas a nombre de las personas investigadas durante el periodo en cuestión. Esto incluye la revisión de todas las transacciones, con especial atención a las transferencias P2P (peer-to-peer) que podrían indicar movimientos de fondos sospechosos.

Administración Federal de Ingresos Públicos (AFIP): declaraciones juradas de bienes personales, impuesto cedular e impuesto a las ganancias de las personas investigadas, con el fin de determinar si han declarado correctamente la tenencia de activos o los ingresos provenientes de transacciones bursátiles.

Información de Terceros: También es necesario obtener información sobre transacciones y tenencias que involucran a terceros, especialmente a través de resoluciones generales del fisco que obligan a los activos virtuales en Argentina a reportar estas actividades. (RG 4614/2019-RG4647/2019- RG5029/2021- RG5512/2024 -RG5348/2023)

Exchanges y Wallets: sobre las transacciones operadas por las personas investigadas, incluyendo tenencias de criptomonedas, datos personales asociados a las cuentas, direcciones IP utilizadas, entre otros detalles relevantes.

c. Análisis y medidas cautelares

Una vez analizada la información recopilada, se han de identificar patrones sospechosos, movimientos de activos, y cualquier indicio de actividades ilícitas. Si se identifican activos que podrían estar en riesgo de ser trasladados o liquidados, es fundamental que el juzgado solicite el congelamiento e inhibición de dichos bienes. Esto asegura que los activos permanezcan disponibles para una posible recuperación o para ser utilizados como evidencia en procedimientos legales. La velocidad en la que congelen o recuperen los fondos siempre es suma relevancia, pero sobre lo es en los casos de los criptoactivos, ya que podrían ser transferidos remotamente por cualquier sujeto que posea las claves y/o contraseñas para operar con ellos.

Este procedimiento asegura un enfoque sistemático y exhaustivo para la recuperación de activos, maximizando las posibilidades de éxito y minimizando la posibilidad de que los activos se pierdan o sean ocultados durante la investigación.

V. Modelos de datos alternativos

La complejidad asociada al uso de los criptoactivos en adición a las características propias de las organizaciones criminales demanda del diseño metodológico de las tareas a llevar a cabo, el que debe incluir planificación de los recursos a utilizar tanto

tecnológicos como materiales y humanos; y el planteo de etapas de abordaje. El uso de nuevas herramientas disponibles se reconoce como una condición necesaria para abarcar este tipo de escenarios.

En este sentido, se propone el uso de la aplicación de la metodología Social Network Analysis (SNA - ARS en su siglas en español), sumado a las nuevas posibilidades de las nuevas inteligencias artificiales, tanto para el reconocimiento preprocesamiento de la información a categorizar, como así también para luego el reconocimiento de patrones a partir de técnicas de aprendizaje automático provenientes de las estadística o de las nueva Ciencias de los datos.

Respecto al análisis reticular, vale aclarar que es tanto una teoría (basada en la teoría de grafos cuyo origen proviene de las matemáticas), una metodología que brinda los investigadores un recetario claro de cómo deberían analizarse los datos de las topologías resultantes de las interacciones de los sujetos en estudio. Y finalmente, también es una herramienta, la cual provee software de muy fácil aprendizaje para su utilización por operadores judiciales. Dicha herramienta permite la rápida generación de indicadores que arrojan luz sobre la importancia de cada sujeto en el contexto de la red investigada. Para ello el SNA, nos otorga indicadores a nivel holístico como lo son las medidas estadísticas de densidad o longitud de una red; medidas de sobre agrupamientos específicos que permiten entre otras cosas determinar subredes -cluster- de una red global más amplia. Y finalmente los indicadores que refieren las medidas de centralidad de cada uno de los participantes del entramado social estudiado.

Por tanto, la propuesta de utilizar el Análisis de Redes está basado en la posibilidad de identificar estructuras que explican la conducta de determinados elementos a partir de sus interconexiones; asimismo, permite extrapolar las vinculaciones de lazos interpersonales a fenómenos de mayor escala (Reynoso, 2011). El SNA permite relevar, mapear y analizar las redes de interacción, destacando nodos/personas y vinculaciones críticas que pueden ser indicativos de actividades ilícitas, puesto que contribuye a procesar datos recabados a partir de una investigación, permitiendo además de los indicadores mencionados una dimensión visual de los mismos, identificar patrones de relaciones que se establecen en el interior de una determinada estructura social, determinar redes existentes y modos de vinculación entre estas (Marsili, 2020)

Por otro lado, la segunda herramienta mencionada en este apartado, específicamente las Inteligencias Artificiales generativas, se ha convertido en un recurso ineludible, tanto para su uso independiente como en combinación con el SNA. Estas tecnologías, cada vez más presentes en nuestra vida cotidiana, representan una herramienta de gran relevancia por su capacidad de aplicación inmediata en las investigaciones criminales. Aunque dejaremos de lado las aplicaciones más complejas debido a las pronunciadas curvas de aprendizaje que requieren, es importante destacar que, en lo que respecta a la estructuración y categorización de información, así como a la generación de descripciones de los valores hallados, las IA populares (*chat-gpt,copilot, gemini, claude*, etc.) nos proporcionan una herramienta poderosa para reducir el tiempo dedicado a tareas de baja complejidad (por supuesto, previa anonimización de todo dato compartido con dichas plataformas).

Dentro de este posible inmediato podemos destacar la posibilidad del análisis análisis de comunicación y específicamente de su contenido:

- Procesamiento de Lenguaje Natural (PLN): La IA puede analizar conversaciones en redes sociales, correos electrónicos y otros textos para identificar lenguaje o términos asociados con actividades criminales. Como así también lo que se denomina “Análisis de sentimientos”: pudiendo las IA evaluar las emociones expresadas en comunicaciones para detectar posibles modos y términos que indiquen o sugieran actos criminales (i.e. actos de habla como por ejemplo lo son la extorsión, la amenaza, etc.)

- Automatización de tareas rutinarias: Muchas tareas repetitivas, como la revisión de videos o la clasificación de datos no estructurados, pueden ser automatizadas, librando de este modo a los operadores judiciales para que puedan concentrarse en tareas mayor complejidad.

- Las inteligencias artificiales articuladas con el SNA, facilitan por ejemplo, y como la hemos dicho, la categorización del contenido de las comunicaciones entre los sujetos de estudio. Esto permite explotar mejor aún las posibilidades que nos otorga el análisis de redes pues, cuando lo deseemos podrían incorporarse dicha informaciòn como datos atributivos en los vínculos, permitiendo no solo un análisis formal y tipológico de la red, sino también robustecer con una caracterización cada tipo de vínculo social establecido en el modelo de datos construido.

VI. Consideraciones finales

La revolución digital y el avance de las tecnologías financieras presentan tanto oportunidades como desafíos en la lucha contra la economía criminal. Ello obedece a que el uso de monedas virtuales contribuye a la materialización de nuevos ilícitos valiéndose de su naturaleza anónima y cambiante, se registran débiles marcos normativos y contables que se adicionan a las brechas tecnológicas existentes.

El uso de criptomonedas ha revolucionado las transacciones financieras, pero también ha abierto la puerta a una variedad de delitos. Desde fraudes y estafas hasta lavado de dinero y extorsión, lo que amplía la complejidad de las investigaciones asociadas a organizaciones criminales, que adicionan desafíos únicos a las autoridades.

Es por ello que las agencias del Estado deben tener mayor grado de especialización y formación en los investigadores, disponibilidad de herramientas digitales específicas y una adecuada interdisciplina en las agencias de regulación, investigación y control.

Es fundamental entonces que las agencias de prevención, regulación y persecución penal adapten sus estrategias y herramientas para enfrentar estos nuevos retos, garantizando una adecuada formación y especialización de sus investigadores, y desarrollando marcos normativos sólidos que permitan una prevención y persecución efectiva de los delitos cometidos con criptoactivos.

Entender las dinámicas que pueden registrarse a través del uso de activos virtuales será clave tanto para desarrollar estrategias efectivas de prevención como para diseñar políticas criminales tendientes a combatir la actividad criminal relacionada con criptomonedas.

En lo que respecto a la investigación de delitos complejos, esta demanda un enfoque multifacético e interdisciplinario que combine técnicas avanzadas de recolección y análisis de datos, estructuras organizativas innovadoras y una colaboración estrecha entre diferentes áreas del gobierno. Solo a través de una planificación meticulosa, el uso de tecnología avanzada y una comprensión profunda de la estructura y funcionamiento de las organizaciones criminales, se pueden enfrentar eficazmente los desafíos que estos delitos presentan al sistema de justicia.

El recupero de criptoactivos, por su parte, se presenta como una oportunidad para fortalecer las áreas de investigación en ciberdelitos, proporcionando recursos financieros necesarios para la adquisición de tecnología y la capacitación de personal especializado.

Otro aspecto en el que el Estado, en relación con las políticas públicas para combatir la criminalidad compleja, debe enfocarse es en el fortalecimiento de las estadísticas sobre estos delitos. Las políticas basadas en evidencia y la transparencia institucional deberían ser la norma, y no excepciones limitadas a informes *ad hoc*. Lamentablemente, en la actualidad, obtener datos sobre la cantidad de delitos, la desagregación por tipo, la cantidad de sentencias relacionadas con criptoactivos, o los montos recuperados de estos activos, es casi tan difícil como rastrear las transacciones de criptoactivos realizadas por las bandas criminales.

Implementar una estrategia integral que abarque tanto el incentivo a la denuncia como la creación de estructuras especializadas dentro del ministerio público como apoyatura transversal a las investigaciones es crucial para enfrentar eficazmente los desafíos que presentan los delitos relacionados con estos.

VII. Glosario

Activo virtual: representación digital de valor que puede comercializar o transferir digitalmente y se puede utilizar para pagos e inversiones.
Blockchain: es la tecnología que hace realidad el sistema, se trata de una base de datos almacenada en forma virtual y donde cada usuario del sistema tiene una copia actualizada y sincronizada. Es un espacio de almacenamiento digital infinito, que independientemente que esté abierto para todos, es de acceso público para todos los usuarios. Esta cadena de bloque elimina la infraestructura centralizada, cada usuario tiene pleno control de sus datos y activos. Podría asemejarse a un libro contable digital, que hace un seguimiento del valor a medida que se mueve de un sitio a otro.
Exchange: son intermediarios en el mercado de las criptomonedas. Se trata de casas de cambio digitales que permiten cambiar dinero fiduciario por criptomonedas o criptomonedas entre sí. Se identifican de dos tipos, aquellas centralizadas o sea controladas por una empresa que custodia esos activos de los usuarios (las claves privadas de los clientes) o descentralizadas o sin control. Las primeras se caracterizan por la aplicación de dos tipos de controles: KYC *"know your customer"* (conoce a tu cliente), es un proceso que identifica y verifica la identidad del usuario y AML *"anti money laudering"*, prevención de blanqueo de capitales o de lavado de dinero; controles que deben realizar las empresas y/o organizaciones para evitar, identificar y reportar posibles conductas sospechosas relacionadas al lavado de dinero o blanqueo de capitales que puedan llevarse a cabo dentro de sus actividades.
Las exchange descentralizadas se caracterizan por ser plataformas que se estructuran sobre una blockchain mediante intercambios directos entre pares (P2P). En este tipo de mercados las comisiones suelen ser nulas, carecen de procesos de KYC y AML.

Token: objeto físico o digital que tiene valor en cierto contexto o para determinada comunidad, aunque su propia materialidad no contenga ese valor en sí. Se generan a partir de piezas de código de programación, en formato de “smart contracts” que corren sobre la blockchain; estos contratos inteligentes son porciones de código de computadoras que determinan las reglas o el funcionamiento de una herramienta o de una plataforma cripto.
Wallet o billetera: cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de las criptomonedas. Entonces, estos monederos digitales operan con dos tipos de claves, una privada y otra pública, ambas se encuentran relacionadas. La clave pública se utiliza para asegurarse de que se es propietario de una dirección que puede recibir fondos, es el código que identifica la cuenta de blockchain. La clave privada es la que otorga la propiedad de los fondos en una dirección determinada, es la verdadera contraseña. Además se utiliza una dirección digital que cumple una función similar a un alias de CBU bancario, esta dirección es la que se envía a terceros para poder recibir las criptomonedas. Existen dos clases de monederos digitales, las billeteras on line, también denominadas caliente o “hot storage” y las off line, de tipo fría o “cold wallet”, cuyas claves se almacenan sin conexión a una red de internet. Estas últimas pueden ser del tipo hardware (similar a un dispositivo USB) o billetera papel, que es una copia impresa de las claves públicas y privadas.

VIII. Referencias bibliográficas

Biscay, P. (2006). La justicia penal y el control de los delitos económicos y de corrupción. Revista Sistemas Judiciales Nro. 11. Recuperado de: https://issuu.com/sistemasjudiciales/docs/sistemas_11

Binder, A. (2013). Ponencia Seminario Internacional: Desafíos actuales y futuros de la persecución penal y de la atención a víctimas y testigos en Chile. Seminarios Organizados por Fiscalía de Chile. Recuperado de: http://www.fiscaliadechile.cl/Fiscalia/Ponencias_Seminario_diciembre_2014.pdf

Davenport, T., & Prusak, L. (1998). Working Knowledge: How Organizations Manage What They Know.

De la Cruz Pinto, M. (2015). La problemática del lavado de dinero y sus efectos económicos sociales. Mecanismos contables para prevenirlo y detectarlo. Córdoba: Universidad Nacional de Córdoba.

Etkin, J. (2006). Gestión de la complejidad en las organizaciones: la estrategia frente a lo imprevisto y lo impensado. Buenos Aires. Editorial Granica.

Editorial Adhoc

Greppi, D. (2022). La tipicidad en la intermediación financiera no autorizada: El artículo 310 del Código Penal. Editorial Adhoc. Buenos Aires.

Marsili, M.; Radyna, N. (2019). Ponencia preparada para el XIV Congreso Nacional de Ciencia Política “La política en incertidumbre. Reordenamientos globales, realineamientos domésticos y la cuestión de la transparencia”. Las ventajas comparativas transitorias en los sujetos que cometen delitos complejos.

Marsili, M., & Radyna, N. (2020). Crimen, Complejidad y Economía. Buenos Aires. Osmar D. Buyatti.

Morin, E. (2009). Introducción al pensamiento complejo. Madrid. Gedisa.

Reynoso, C. (2011). Redes sociales y complejidad: Modelos interdisciplinarios en la gestión sostenible de la sociedad y la cultura. Universidad de Buenos Aires. Buenos Aires.

Salcedo-Albarán, Eduardo & Garay-Salamanca, Luis & Gómez, Francisco & Ugaz, José & Sullivan, John & Bunker, Robert. (2016). Macro-criminalidad: Complejidad y Resiliencia de las Redes Criminales.

Silva, G., Feser, M. E., Santos, M., & Ferreiro , J. (2023). Criptomonedas y delitos complejos: hacia una nueva perspectiva de su impacto en la investigación criminal . *Minerva*, *2*(6), 6–19. Recuperado de https://ojs.editorialiupfa.com/index.php/minerva/article/view/118