Martínez, Alejandro Manuel

Análisis de redes, comunicaciones telefónicas e investigación penal

Alejandro Manuel Martínez, Repositorio Institucional Digital de Acceso Abierto,
Noviembre de 2020, pp. 65,
http://ridaa.unq.edu.ar,
Universidad Nacional de Quilmes, Secretaría de Posgrado,
Especialización en Criminología

Análisis de redes, comunicaciones telefónicas e investigación penal

Trabajo final integrador

Alejandro Manuel Martínez

martinezale1987@gmail.com

Resumen

El cruce de información telefónica constituye un procedimiento central en las investigaciones criminales complejas. Los datos comúnmente analizados por las fuerzas de seguridad o los agentes judiciales refieren a los interlocutores, la fecha y hora, la duración, la ubicación y el sentido de una comunicación. Si bien los procedimientos utilizados comparten el objetivo común de analizar las personas investigadas y sus contactos, en términos metodológicos existe un abanico de implementaciones, desde los enfoques artesanales hasta la manipulación de software especializado.

A mi entender, los análisis de telecomunicaciones tienen problemáticas acuciantes en el plano metodológico. Por un lado, los trabajos artesanales que utilizan exclusivamente la potencia de cálculo de la mente humana están limitados en cuanto a su eficacia temporal y en la falta de garantía en el control de propagación de errores. Por el otro lado, aquellos softwares de cruce de datos, si bien agilizan los procesos, también constituyen una especie de “caja negra” que ubica en un segundo plano las consideraciones analíticas que son ineludibles para el investigador. Las dificultades de ambos abordajes se potencian bajo el nuevo contexto de la “big data” que impacta de forma directa en el ámbito de la investigación penal.

Ante este panorama, mi aporte consiste en documentar los conocimientos extraídos de mi experiencia laboral en una oficina judicial denominada Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP), dependiente de la Procuración General de la Nación. Allí, el equipo interdisciplinario al cual pertenezco utiliza los fundamentos científicos del análisis de redes sociales (ARS o SNA por sus siglas en inglés) aplicado al estudio de datos asociados a las telecomunicaciones en el marco de investigaciones penales. Pretendo con ello aportar en la estandarización de los procesos, que sean reproducibles y trazables, y que vuelvan a poner en primer plano la pericia del investigador de forma independiente al software utilizado.

ANÁLISIS DE REDES, COMUNICACIONES TELEFÓNICAS E INVESTIGACIÓN PENAL

Un aporte metodológico en análisis de inteligencia criminal

Trabajo Final Integrador
Especialización en Criminología
Universidad Nacional de Quilmes

Autor: MARTINEZ, Alejandro Manuel
Director: MICELI, Jorge Eduardo

Índice de contenidos

1 - Introducción

1.1 - Descripción del problema y justificación del contexto

Las últimas décadas presentaron cambios tecnológicos profundos a nivel mundial. El surgimiento de internet, la difusión de las computadoras personales y la utilización de dispositivos móviles por nombrar solo tres de las más importantes transformaciones tecnológicas, tuvieron como consecuencia que los individuos generemos datos de cada una de nuestras prácticas sociales, incluidas las delictivas o criminales. Estos cambios de época determinaron consecuencias que deberían reformular muchos aspectos de la investigación penal. En ese sentido, juristas como Guariglia, Director de la División de Enjuiciamiento y Apelaciones de la Fiscalía de la Corte Penal Internacional, afirman que:

> "nadie discutirá que no se puede ingresar a la era del Big Data con un expediente cosido a mano. Aun cuando haya habido algunos avances puntales en el uso de tecnología por parte de la persecución penal, esto es insuficiente para el doble fin de cubrir la brecha tecnológica que nos separa de los sistemas más modernos de investigación y persecución penales, por un lado, y de dotar al ministerio público de las técnicas y tecnologías necesarias para investigar eficientemente formas complejas de criminalidad" (Guariglia, 2016: 7).

Estas opiniones invitan a pensar cómo se investiga penalmente en Argentina. Imagínese por un momento la situación cotidiana de un operador judicial que tiene que impulsar casos de distintas temáticas. A su vez, intenté dimensionar el volumen de datos potenciales de una causa: testimonios, allanamientos, información documental, escuchas telefónicas, informes periciales, entre otras medidas de prueba. Ante esta situación, Guariglia se expresa contundentemente: "*un punto de partida fundamental debería ser, en verdad, un reconocimiento: en Argentina, o al menos, en el ámbito de la administración de justicia nacional (en sentido amplio), no se investiga bien, ni hay estructuras aptas para ello – o al*

menos, no se investiga en forma adecuada a las posibilidades y los desafíos de este siglo" (Guariglia, 2016: 1).

¿A qué se debe esta descripción? La respuesta debería ser multicausal sin lugar a dudas. Un eje central para comenzar a abordarla es entender que nos *sobran datos* pero nos *falta conocimiento* o, en otras palabras, que debemos incorporar procedimientos, metodologías y perspectivas que permitan abordar esta situación. Para Navarro y Bonilla,

> "acumular información no supone tener más conocimiento y procesar información no es lo mismo que aprovechar el conocimiento. En realidad, estamos saciados de información, pero hambrientos de conocimiento" (Navarro y Navarro Bonilla, 2003: 272).

La descripción de ese contexto, debo advertirlo, me resulta familiar. El interés de este proyecto está vinculado con mi desempeño profesional dentro del Ministerio Público Fiscal de la Nación. Mi área de trabajo se denomina Laboratorio de Análisis de Telecomunicaciones y depende orgánicamente de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP) de la Procuración General de la Nación. Allí trabajé de forma constante con ciento de miles de registros de comunicaciones en donde resultaba evidente que se acumulaba muy rápido información pero que no existían metodologías para procesar y analizar sus datos.

Dicha experiencia laboral me permitió tener acceso de primera mano a las solicitudes y necesidades de los instructores de las causas penales. En ese sentido, junto a un equipo de trabajo interdisciplinario fui parte del estudio, desarrollo y estandarización de una metodología de trabajo para realizar cruces de información telefónica en causas de narcotráfico, trata con fines de explotación sexual, secuestros extorsivos, robos, homicidios y lavado de activos. Nuestra misión consistía en aprovechar la multiplicidad de datos, analizarlos y generar nuevas instancias de conocimiento para fortalecer las hipótesis de acusación fiscal.

Allí comprendí que, para los sumariantes judiciales, el tratamiento y el análisis de la información de telecomunicaciones puede ser útil en tres instancias diferentes. En un primer lugar, el horario de una comunicación, el espacio de cobertura de una celda en la que impactó una llamada o la frecuencia de mensajes a determinados abonados pueden evaluarse como información heurística relevante para desarrollar la instrucción de una causa. En este sentido, el análisis de telecomunicaciones constituye una fuente de *insight* muy utilizado en los momentos preliminares de una pesquisa.

En una segunda instancia, el estatus de dicha información puede ser clave para demostrar o descartar una hipótesis. Aquí la información pasa a ser considerada como *prueba* directa o indirecta vinculada con la hipótesis de acusación fiscal.

Por último, existe un tercer momento en donde la información de telecomunicaciones necesita ser visualizada de forma clara y concisa al momento de juicio. La función principal en esta instancia es la de generar *convencimiento* en el juez o tribunal, producto de utilizar otros soportes de forma complementaria a la oralidad de los alegatos.

Ahora bien, la generación de metodologías para desarrollar el insight, la prueba o el convencimiento requieren de un conocimiento comunicable y, por ende, formalizado. Sin embargo, la situación institucional general parece ser otra ya que

> "el conocimiento se produce y comunica en una organización mediante un ciclo que comienza y finaliza con la creación de conocimiento tácito por los diferentes individuos que la componen. El conocimiento tácito es de posesión personal, difícil de formalizar y de compartir, sólo accesible a los otros de modo indirecto" (Navarro y Navarro Bonilla, 2003: 272).

Justamente, mi propósito es empezar a revertir esta situación realizando un proyecto de innovación orientado al desarrollo de procesos tanto explícitos como trazables y, por ende, a aumentar los estándares de reproducción y comunicabilidad necesarios en este tipo de análisis.

Para ello, esta tesina está organizada en dos secciones. En la primera parte se presenta el marco teórico utilizado para el trabajo. El mismo está compuesto por dos capítulos: uno

relacionado con la perspectiva del análisis de la inteligencia criminal y el segundo con el enfoque de análisis de redes sociales. En éste último capítulo se presenta una introducción al ARS, se desarrolla un estado del arte respecto al maridaje del ARS con la investigación penal y finaliza con una exposición de aquellos trabajos que vincularon ARS con el análisis de telecomunicaciones.

En la segunda sección se presenta el desarrollo del problema de investigación, su análisis y un ejemplo de aplicación. Este apartado cuenta con tres capítulos: el primero trata de la recolección de datos sobre telecomunicaciones, el segundo sobre la preparación y procesamiento de los datos y el tercero sobre el ARS y su aplicación a un caso real.

Finalizo esta tesina con algunas conclusiones sobre los puntos fuertes de esta perspectiva como así también con algunas dificultades y desafíos que hay que atravesar en un futuro, con el objetivo de consolidar herramientas confiables de inteligencia criminal.

1.2 - Objetivos generales

- Fundamentar la utilización del análisis de redes sociales como método para el análisis de comunicaciones telefónicas en investigaciones penales.

1.3 - Objetivos específicos

- Describir los aportes criminológicos del análisis de redes sociales a la investigación penal.
- Ponderar las dificultades y desafíos del análisis de redes sociales aplicado a la investigación penal.
- Describir las fuentes y los procesos para trabajar con información asociada a las telecomunicaciones en el marco de una investigación criminal.
- Presentar las principales técnicas del ARS y aplicarlo a un ejemplo de análisis de telecomunicaciones.

2 - Marco Teórico

2.1 - La perspectiva del análisis de inteligencia criminal

> *"La primera pregunta a la cual debemos responder es por qué en inteligencia se utiliza como método de trabajo el correspondiente a las ciencias sociales. La respuesta es porque el delito, ya se lo interprete como una conducta desviada, anomia, acción antijurídica, etc., es un fenómeno que se produce en el seno de la sociedad e involucra a personas y sus interrelaciones" (Enrique Galessio).*

La propuesta de este trabajo se enmarca en el análisis de inteligencia criminal entendido como el punto de encuentro entre los procedimientos propios de las ciencias sociales y su aplicación a la investigación penal. El propósito de la inteligencia criminal es aumentar la eficiencia de los órganos judiciales y policiales en materia de seguridad aplicando técnicas superiores a las empleadas en la investigación del delito común. En ese marco, la inteligencia criminal se debería utilizar específicamente en el análisis del delito de naturaleza organizada y no a los llamados delitos comunes. Esta distinción es importante para descartar del análisis aquellos delitos oportunistas o aislados y enfocarse en aquellos intencionalmente organizados, desarrollados y ejecutados por más de dos personas.

El núcleo del análisis de inteligencia criminal sostiene que la inteligencia no proviene de la recolección y el manejo de información. La información solo es la condición necesaria mas no la suficiente para generar inteligencia. Ésta se entiende mejor como el resultado final de un proceso de generación de información sumado a técnicas y metodología de análisis de los datos. Solo en los últimos tiempos esta perspectiva fue explorada e incorporada en las investigaciones penales. De hecho, "hasta hace relativamente poco tiempo atrás en nuestro país, pocas policías provinciales eran capaces de producir inteligencia criminal, ya que el componente analítico usualmente faltaba" (Pezzuchi, 2017).

El análisis de inteligencia criminal responde a las preguntas del estilo ¿quién?, ¿qué? y ¿con quién? al analizar eventos delictivos. El eje central lo constituyen las relaciones entre personas y organización involucradas en actividades de naturaleza organizada. Con estas preguntas, el analista de inteligencia criminal busca entender la estructura y jerarquía interna de las organizaciones delictivas, los flujos de bienes, dinero o información, las relaciones entre los participantes y su dinámica, con el objetivo de la detención y enjuiciamiento de las personas involucradas. Por ello, en el análisis de inteligencia criminal se aplican diversas

> "técnicas que enlazan (relacionan) personas con personas, personas con organizaciones, y organizaciones con organizaciones. Se realizan análisis de comunicaciones telefónicas para entender la estructura y la forma de operar de la organización, al igual que análisis de transacciones financieras para determinar los flujos monetarios y la disposición de efectivo y bienes por parte de las organizaciones delictivas" (Pezzuchi, ----: 33).

Para llevar adelante este tipo de investigaciones resulta importante tener presente algunos de los pasos del ciclo de inteligencia criminal (Navarro y Navarro Bonilla, 2003). En primer lugar, me gustaría mencionar la "toma de datos", momento que trata sobre la adquisición y reunión de datos en bruto que, en el ámbito de las telecomunicaciones, pueden provenir de tres fuentes distintas[1]: a) la interceptación de comunicaciones; b) la extracción forenses de celulares; y c) la solicitud de registros de comunicaciones a las empresas prestatarias de servicios telefónicos. Si bien en un nivel de abstracción esta información resulta de la misma naturaleza, su presentación se manifiesta de diversas formas, sobre todo con el punto c) vinculado a cómo dan sus respuestas las prestatarias.

Ante esa dificultad, cobra relevancia la etapa de procesamiento de la información. Si bien en este trabajo no me interesa desarrollar el detalle operativo de cómo tratar con tipos de datos diferentes, lo cierto es que esta instancia de normalización de la información requiere de transformaciones conceptuales que indicaremos y que, en nuestra labor cotidiana, las aplicamos técnicamente con la utilización de bases de datos relacionales.

[1] Más adelante se tratará de forma específica los tipos de datos que se pueden obtener como así también una descripción de ventajas y desventajas de cada tipo de fuente.

Finalmente, dentro del ciclo de inteligencia me interesa desarrollar su cuarta etapa, es decir, la de análisis y producción, entendiéndola como el momento en donde se extrae con precisión y rapidez conocimiento a partir de los datos previamente estructurados. Según las palabras de Navarro y Navarro Bonilla,

> "esta fase marca la frontera entre información e inteligencia, que se manifiesta dentro de las estructura de los servicios de inteligencia en la separación entre los órganos responsables de la obtención de información y los encargados de su elaboración en función de sus áreas de actuación (nacional, internacional, etc.) mediante el trabajo de analistas que aplican todo su capital intelectual" (Navarro y Navarro Bonilla, 2003: 276).

Este marco de inteligencia criminal se encuentra en franco crecimiento a lo largo de las agencias judiciales y de seguridad de numerosos países (Chen et al, 2004; Britos et al, 2008). Siguiendo la noción de que el objetivo de la explotación de información es descubrir patrones interesantes a partir de grandes volúmenes de datos almacenados, se puede entender al análisis de redes sociales como una de las técnicas principales de minería de datos aplicadas a la investigación penal (Chen et al, 2004: 52). Siguiendo los términos anteriores, entiendo el análisis de redes sociales como una perspectiva tanto metodológica como epistemológica que se puede integrar de forma relevante dentro del campo del análisis de inteligencia criminal.

2.2 - El enfoque del análisis de redes sociales

2.2.1 – Introducción

Como fue mencionado, la perspectiva metodológica central de este trabajo es el Análisis de Redes Sociales (de ahora en más ARS) y por eso resulta importante demarcar conceptualmente en qué consiste. En primer lugar, el ARS no tiene vínculo directo con el uso de sentido común asociado a la difusión masiva de plataformas como Facebook, Twitter,

Instagram, Whatsapp, Telegram, entre muchas otras. En segundo lugar, tampoco tiene que ver con el uso metafórico aplicado en trabajos periodísticos, de ciencias sociales o del discurso penal, en donde con frecuencia se pueden leer nociones como "entramado social", "red delictiva", "red mafiosa", "red clientelar", entre otras. Las mismas refieren a la existencia de una red que está operando en un marco empírico, pero no se puede encontrar una definición de sus componentes, una descripción de su estructura o un análisis de su dinámica.

Por el contrario, estas últimas características se explicitan en el ARS en términos estrictos. El uso formal de la red se puede definir entonces como un modelo compuesto por elementos denominados "nodos" vinculados entre sí por "lazos" o "aristas". Entre sus cualidades cabe destacar que 1) por su nivel de abstracción resulta independiente de marco teórico y referencia disciplinar; 2) no presentan positividad o negatividad en términos éticos o políticos; 3) no se pueden reducir al funcionamiento técnico de un software ya que implican reflexiones metodológicas y epistemológicas profundas.

El origen histórico del ARS se puede remontar al siglo XVIII, cuando el matemático suizo Leonhard Eüler desarrolló lo que se conoció como "teoría de grafos" para resolver el famoso problema de los puentes de Königsberg. Este momento fundacional de la teoría de grafos continuó desarrollándose hasta el presente: sin entrar en detalles que no hacen al tema de exposición de este trabajo, hay que hacer justa mención a los aportes de la sociometría de Jacob Moreno, a la teoría de grafos aleatorios de Paul Erdös y Alfréd Rényi, a la implementación pionera del análisis de redes en antropología de la Escuela de Manchester o en sociología con el enfoque de la "fuerza de los lazos débiles" de Mark Granovetter. Ya para mediados de la década del 90, con la difusión de las computadoras personales y el desarrollo de los primeros softwares especializados en redes, surge lo que se conoció como "modelo canónico" del ARS a través del trabajo de Stanley Wasserman y Katherine Faust. En la actualidad, los tópicos centrales de un estado del arte refieren al análisis de las llamadas redes libres de escala de Lázló Barabási y a las investigaciones sobre la propiedad de "mundos pequeños" del sociólogo Duncan Watts y del matemático Steven Strogatz[2].

[2] Para un análisis histórico y epistemológico de estos conocimientos orientado a científicos sociales, ver el exhaustivo trabajo del antropólogo Carlos Reynoso (Reynoso, 2011).

El detalle que hay que rescatar de esta enumeración es su interdisciplina, una cuestión característica del análisis de redes. En efecto, la interdisciplina del ARS se manifiesta de dos formas: en primer lugar, en un sentido histórico, puesto que tanto en el desarrollo de sus conceptos como en la resolución de sus problemas participaron científicos provenientes de disciplinas exactas, naturales y sociales, desde matemáticos y físicos hasta antropólogos, sociólogos y psicólogos. Por otra parte, la interdisciplina también está dada por sus múltiples objetos empíricos de estudio ya que existen trabajos de las más variadas ramas que aplican alguno de los temas del análisis de redes.

Como ya enunciamos, una red es en términos simples un conjunto de elementos denominados "nodos" conectados por "lazos". La definición de qué es un nodo y de qué es un lazo corre por cuenta de la persona que está investigando y la única regla que hay que respetar es que los nodos y los lazos siempre correspondan a los mismos criterios de definición elaborados. A diferencia de los enfoques estadísticos donde importan las entidades y sus variables, en el ARS lo que cobra relieve son las entidades y sus relaciones. En otras palabras,

> "la mayor diferencia entre los datos atributivos y los reticulares es que los datos convencionales se centran en actores y atributos mientras que los datos de red se centran en actores y relaciones. La diferencia es importante para las decisiones que el analista debe tomar en el diseño de la investigación, en el registro de datos, el desarrollo de mediciones y su interpretación" (Hanneman, 2000:6).

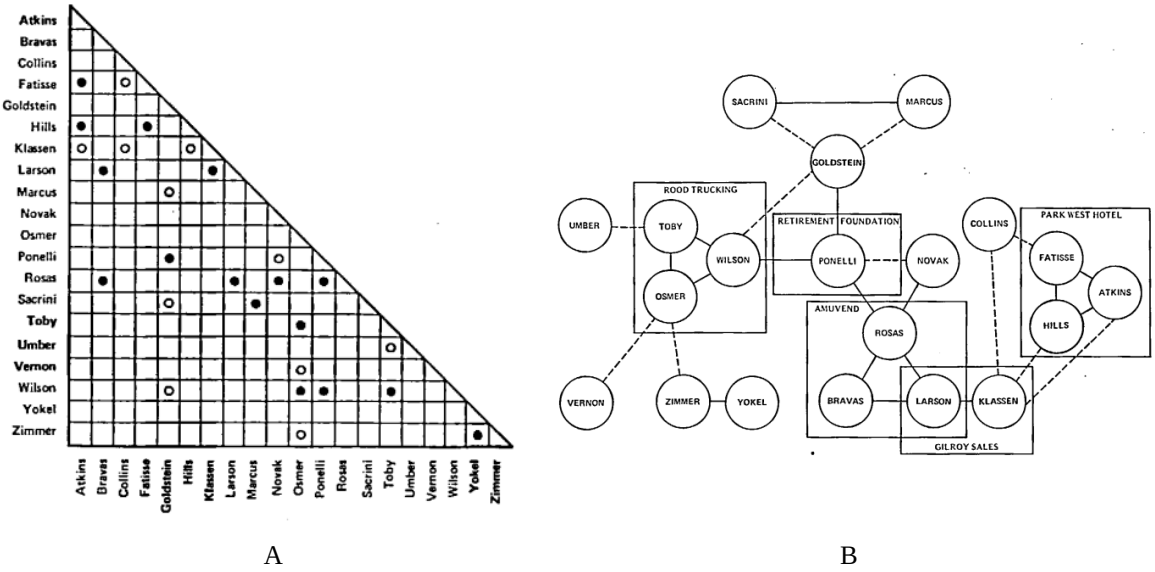
Un especialista conforma una red de forma explícita operacionalizando sus componentes y aplicando un esquema metodológico para recolectar los datos. En una segunda instancia, ya con la red conformada, sobreviene el análisis de la misma. Los algoritmos del ARS constituyen una parte central del análisis que permite describir ciertas características que generalmente resultan contraintuitivas y, por ende, una poderosa fuente de información nueva que se encontraba latente en la base de datos previa. En términos generales, los indicadores brindados por los algoritmos del ARS se utilizan para describir la estructura del grafo, su dinámica y comportamiento a la vez que permite identificar nodos centrales, conexiones o vínculos importantes y subgrupos dentro de la red.

2.2.2 - El ARS y la investigación penal

Ante las posibilidades que presenta la perspectiva epistemológica y el sólido aparato técnico, la unión entre el ARS, la investigación penal y la reflexión criminológica no tardó en aparecer. Desde la década del 70 se registran trabajos pioneros como el de Walter Harper y Douglas Harris en donde se aboga por la aplicación del *"link analysis"* como técnica de la inteligencia policial útil para prevenir y controlar al crimen organizado (Harper y Harris, 1975). Este texto resulta muy interesante por tratarse de un mosaico entre pasado y presente. Por un lado la visualización de las redes utiliza los gráficos de ANACAPA, una forma de visualizar los datos que hoy en día resulta arcaica[3]. Tampoco se presentan métricas surgidas de los algoritmos del ARS por obvias razones de desarrollo tecnológico.

Sin embargo, por otro lado llaman la atención la constancia y actualidad en la presentación de los problemas y en la elaboración conceptual de sus propuestas. En ese sentido, los autores describen los aportes del ARS en términos cercanos al consenso experto actual como, por ejemplo, la potencialidad de integrar múltiples fuentes y grandes volúmenes de información dentro del modelo, la capacidad de desarrollar hipótesis de investigación y la identificación de puntos débiles o figuras centrales para la intervención de la red criminal. También resulta importante a los fines de este trabajo porque es el antecedente más antiguo que encontré en donde se menciona la posibilidad de adoptar el ARS aplicado a registros telefónicos (Harper y Harris, 1975: 158).

[3] Dichos gráficos debían respetar tres reglas: 1) la proximidad espacial entre dos nodos indicaba la cercanía real dentro de la organización criminal; 2) la posición de los nodos debía ser específica para que los lazos no se crucen entre sí y; 3) el espacio central del gráfico estaba reservado para el nodo central de la organización criminal.



A B

Figura 1 – A: Matriz de asociación de personas en donde se identifican con círculo negro los vínculos fuertes y con blanco los vínculos débiles. La falta de círculos en la intersección de dos personas representa la ausencia de vínculo. B: gráfico de ANACAPA en donde se identifican a las personas (círculos) y sus relaciones fuertes (línea recta) o débiles (línea punteada) junto a las organizaciones que integran las personas (rectángulos). Fuente: Harper y Harris, 1975.

A pesar de este antecedente, no pocos autores identifican el maridaje moderno entre el ARS e inteligencia criminal con la obra de Malcolm Sparrow a comienzos de los noventa (Krebs, 2002a; 2002b; Wiil, 2013; Morris y Deckro, 2013; Duijin y Klerks, 2014; Burcher y Whelan, 2017). Desde la introducción de su artículo, el autor sostiene que

> "las agencias de inteligencia, a pesar de sus obvias coincidencias sobre la importancia del análisis de inteligencia, han permanecido en su mayor parte relativamente poco sofisticadas en la utilización de herramientas analíticas y conceptuales. Normalmente tienen muchos datos, la mayoría computarizados, pero comparativamente poca capacidad para extraer inteligencia útil de ellos." (Sparrow, 1991: 251)

En ese trabajo, Sparrow realiza una enumeración de las distintas aplicaciones conceptuales y tecnológicas en términos de red asociadas con la investigación penal, y destaca como

antecedentes directos del ARS al mencionado "link analysis" y los "ANACAPA charts". Pero describe también sus límites al sostener que el objetivo último de estas técnicas es el de la "ayuda pictórica" y que, en última instancia, el análisis de inteligencia continuaba dependiendo de procedimientos artesanales y heurísticos de los analistas. En este sentido, el texto de Sparrow es el primer intento serio de dejar atrás una visión simplista del análisis reticular aplicado a la inteligencia criminal y pegar el salto teórico y técnico que la ciencia de las redes ya estaba evidenciando en otros ámbitos[4].

A su vez, el autor abogaba por la búsqueda de un mayor interés por parte de los científicos de redes sobre los desafíos específicos de las redes criminales. Es así como Sparrow afirma que los investigadores de redes desarrollaron herramientas en el contexto de redes pequeñas, estáticas y de un solo tipo de vínculo. Sin embargo, las redes criminales presentan cuatro especificidades (o problemáticas) que todo analista de redes tiene que enfrentar al momento de realizar inteligencia criminal.

> 1) el tamaño de la red: las bases de datos de inteligencia criminal pueden ser verdaderamente enormes, con miles de nodos y lazos. Las consecuencias computacionales del tamaño de una red no son para menospreciar.
>
> 2) la incompletitud de la red: que los actores de una red criminal se preocupen por no dejar rastros de sus elementos parece una verdad de perogrullo, pero sus efectos plantean interesantes problemas teóricos relacionados con la posibilidad de realizar inferencias, interpretar métricas o tomar líneas de acción. No hay que olvidar que los datos disponibles corresponden más a las líneas de investigación y los juicios

[4] Sparrow realizó incisivas críticas a las reglas que debían respetar los gráficos ANACAPA utilizando conocimientos técnicos de estadística y teoría de grafos. En torno a la regla de proximidad criticó su simpleza artesanal existiendo abordajes específicos como las técnicas de agrupamiento o el escalamiento multidimensional de datos reticulares; sobre la regla de que las aristas no se crucen indica que sería necesario que la organización criminal fuera planar lo cual resulta una exigencia ridícula; y sobre la noción de centralidad le resulta poco relevante al asociarse con la centralidad de grado, dejando de lado métricas más complejas de centralidad (ver Sparrow, 1991: 256).

anteriores de los agentes policiales o judiciales más que a la realidad objetiva de la organización criminal.

3) los límites difusos de la red: no existen reglas objetivas para determinar los puntos de corte de una red. La mayoría de las veces los límites son ambiguos y lo que mejor puede hacer el analista es aceptar la arbitrariedad del recorte haciéndola explícita.

4) la dinámica de la red: ninguna red es estática, todo el tiempo se encuentra cambiando. Generalmente resulta más fácil y comunicable la información reticular sumarizada, sin embargo, dicha práctica deja de lado la evolución de las redes. Más que evaluar la presencia o ausencia de un lazo, Sparrow recomienda analizar cuándo estos se cortan o van menguando su fuerza a lo largo del tiempo.

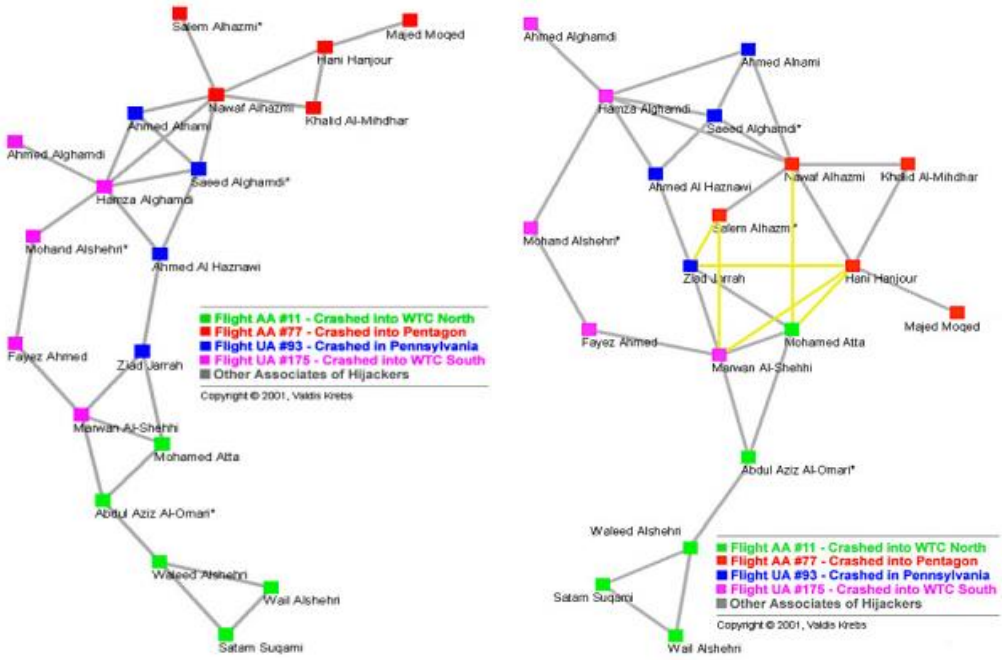
Si bien el trabajo de Sparrow significó una apertura programática desafiante, durante la década del 90 no se registraron trabajos académicos que traten la vinculación entre el ARS y la criminología o el campo penal. Hubo que esperar al cambio de milenio para que el desarrollo tecnológico y el nuevo contexto mundial después de los atentados a las Torres Gemelas dieran lugar a la consolidación del ARS como herramienta. Según Miceli, Orsi y Rodríguez García, el impacto de las organizaciones de tráfico de drogas por un lado y las terroristas por el otro, sumado a la nueva perspectiva para aprehenderlos,

> "derivaron en la generación de un importante caudal de reflexiones respecto de la capacidad del funcionamiento en red de organizaciones y personas para producir, como propiedad emergente, comportamientos colectivos que incluso parecen escaparse de lo predecible. En lo que toca al campo penal, el ARS quedó, así, inicialmente asociado a un conjunto delimitado de fenómenos -integrado, básicamente, por distintos tipos de sujetos grupales clandestinos y violentos-: este proceso de síntesis, con sus más y sus menos, probó sin embargo el potencial del enfoque para la investigación de toda clase de 'delito complejo'." (Miceli et. al, 2016:24)

Los trabajos que más impacto y repercusión tuvieron en esta instancia fueron sin lugar a dudas los de Valdis Krebs sobre la red terrorista de Al-Qaeda, responsable de los atentados

del 11 de septiembre del 2001 en Estados Unidos (Krebs, 2002a; 2002b). Si se evalúa en cantidad de citas, los trabajos de Krebs tienen similar influencia en los textos que vinculan ARS e inteligencia criminal que los de Sparrow. De todas formas, existe una diferencia sustancial entre ambos productos: mientras que el aporte de Sparrow fue realizar la fundamentación teórico-programática, el trabajo de Krebs fue de implementación, es decir, eminentemente empírico y práctico.

A meses de los atentados del 11 de septiembre del 2001, la prensa empezó a utilizar constantemente el concepto de "red terrorista" y a asociarlo con las características de "amorfo", "invisible", "dispersa" o "resiliente". Ante esta situación, el objetivo de Krebs fue visualizar de la forma más realista posible la estructura de la red terrorista que llevó adelante los atentados (Krebs, 2002a; 2002b). Para ello recolectó la información pública que aparecía en los medios, la procesó considerando el grado de veracidad y la ponderó teniendo en cuenta la noción de "confianza previa" al momento de incorporar nuevos integrantes a la red. Esta idea la operativizó construyendo lazos de tres tipos de fuerzas ponderados por la cantidad de tiempo juntos de cada par de integrantes de la red. Por ejemplo, aquellos que vivieron juntos o estudiaron en los mismos institutos educativos tienen un lazo ponderado más fuerte que aquellos que sólo compartieron una reunión o realizaron una transferencia financiera.



A B

Figura 2 – A: Red de contactos de confianza previos del grupo terrorista de Al-Qaeda antes de la implementación de los atentados de septiembre del 2001. B: Red de contactos de confianza previos junto con nuevos integrantes y vínculos a partir de reuniones en días previos a los atentados. (Krebs, 2002a).

Lo que se desprende del análisis de Krebs es la relación inversa entre eficiencia de la organización y encubrimiento de la misma. El indicador utilizado del ARS fue la longitud media de camino, la que para el autor resulta bastante alta teniendo en cuenta la poca cantidad de nodos identificados. Esta dispersión del grupo terrorista fue tal que en un mismo avión los integrantes de grupo se encontraban a dos pasos de distancia uno del otro. Por otra parte, en momentos previos al atentado, cuando las necesidades operativas, de coordinación y reporte ascienden, se concretan reuniones en donde se generan nuevos nodos y vínculos. Esto aumenta la conectividad de la red reduciendo significativamente la longitud media de camino (Krebs, 2002a: 46).

Luego de estos desarrollos, el ARS empezó a abarcar una casuística de diversas formas de "criminalidad organizada". Desde el nuevo milenio hasta la actualidad, con los avances tecnológicos y el nuevo contexto mundial después de los atentados a las Torres Gemelas, la

expansión del ARS como herramienta de inteligencia criminal se consolidó abarcando múltiples aspectos. Tal como Krebs y sus trabajos sobre Al-Qaeda, los desarrollos con ARS empezaron a incorporar análisis empíricos cada vez más amplios: terrorismo (Krebs, 2002a, 2002b; Hopkins, 2010; Karthica y Bose, 2011; Agarbar, 2018), narcotráfico (Morselli, 2010; Calderoni, 2012), actividades mafiosas (McGloin 2005; Papachristos, 2009), crimen organizado (Klerks, 2001; Chen et al, 2004; van der Hulst, 2009), comunidades criminales (Lu et al., 2010; Sarvari et al, 2014), entre muchos otros tópicos. El estudio más completo en lengua española sobre la aplicación del ARS al estudio de delitos complejos es el del antropólogo Jorge Miceli y los abogados Omar Orsi y Nicolás Rodríguez García (Miceli et. al. 2016).

La generación de esta casuística consolidó la perspectiva del ARS en el ambiente de la inteligencia criminal al punto de que se pueden contabilizar no pocas contribuciones criminológicas. Entre ellas podemos mencionar las siguientes:

1) La relevancia de las interacciones débiles

La perspectiva del sociólogo Mark Granovetter sobre la "fuerza de los lazos débiles" tiene su interpretación en el esquema de las redes criminales. Recordando el principio de Sparrow de que por definición las redes criminales son "oscuras" o "secretas" se llegó al consenso de que las organizaciones criminales más profesionales son aquellas que mantienen sus lazos principales escasamente activados. Esta idea fue desarrollada por Baker y Faulkner al afirmar que

> "Various practices and organizational devices are used to protect a secret society. Members may conceal the secret society and their involvement in it by limiting face-to-face interaction. Leaders, for example, may be unknown to ordinary members (Simmel 1950, pp. 371- 72). Members can increase protection by minimizing the channels of communication (Goffman 1970, p. 78; Fitzgerald 1973, p. 260)." (Baker y Faulkner, 1993: 843)

De forma complementaria, Miceli, Orsi y Rodríguez García sostienen que en la conformación de una red criminal sofisticada el mecanismo de desarrollo no parece ser una "estructura de relaciones densa y de confianza extrema -en la cual todos sus miembros se conocen con una

intensidad comparable-" sino más bien "un tipo de entramado en el cual algunos pocos miembros son capaces de conjugar y coordinar las acciones del resto de los integrantes, fijando objetivos acotados y específicos, cuya información no se comparte" (Miceli et. al., 2016:51).

Si bien es cierto que el nivel de organización de un grupo criminal tiene un abanico de posibilidades muy amplio entre lo simple y lo complejo, la idea central aquí es que las interacciones débiles en una organización criminal parecen ser una condición indispensable para balancear las necesidades entre eficiencia operativa y riesgos de que se desvele el secreto.

2) La detección sofisticada de entidades centrales o "key players"

Si en el punto anterior se enfoca en los tipos de lazos, acá se pone la mirada en el análisis de los nodos de una red, constituyendo el reverso de una moneda. Teniendo en cuenta que la dirección de una organización criminal es muy consciente de la necesidad de invisibilizar su rol estructural para no ser detectado, es que hace ya mucho tiempo que el grado nodal se considera como una métrica muy simple para determinar la centralidad de un nodo dentro de una red.

Para autores como Calderoni, la centralidad de grado, a contramano de indicar importancia dentro de una organización, identifica a las personas más vulnerables de las mismas por estar más expuestas a la mirada del sistema penal de justicia.

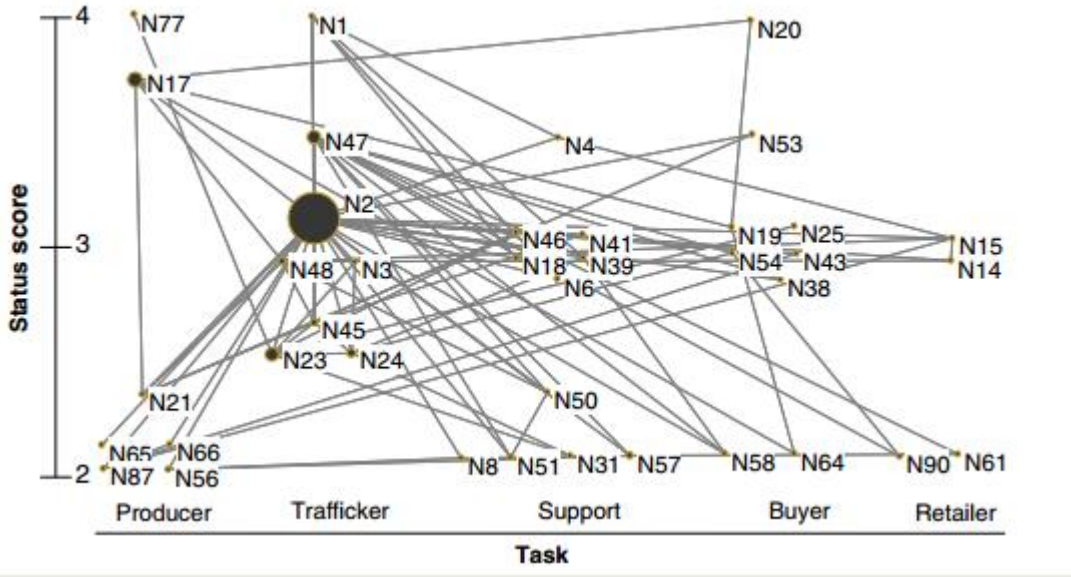


Figura 3 - Red de la organización narcotraficante de Chalonero en Italia. En el eje horizontal se indican los roles de las personas investigadas mientras que en eje vertical se mide su status El tamaño menor o mayor de los nodos está en función de la centralidad de grado. Se puede observar como ninguno de los nodos de mayor status presentan altos niveles de centralidad. (Calderoni, 2012:344)

En otras palabras, para organizar y concretar las actividades criminales, generalmente los grandes jugadores no son los que mayores vínculos presentan, sino aquellos cuya posición en la red determinada por los lazos sea de mayor calidad. Varios algoritmos fueron diseñados para intentar aprehender otras características más sutiles o antiintuitivas como, por ejemplo, la centralidad de intermediación:

> "In general, degree centrality reflects active involvement in group activities, but in the case of criminal networks it can also be interpreted as a sign of vulnerability. From this perspective, betweenness centrality may reveal more strategic positioning within a network, ensuring less visibility while allowing control to be maintained over the flow of information". (Calderoni, 2012: 333)

La centralidad de intermediación garantizaría, en términos de Calderoni, una posición de intermediario dentro de una organización criminal. Se considera que aquellos nodos con mayor grado de intermediación cumplen un rol importante para el funcionamiento de la organización y el flujo de la información, por lo que se trataría de nodos de un status o rango intermedio. Sin embargo, en no pocas redes criminales los líderes de la organización no son identificados ni por la centralidad de grado ni por la centralidad de intermediación.

En ese sentido, una cuestión interesante es que no solo se desarrollaron una pluralidad de algoritmos, sino que también se realizaron interpretaciones importantes sobre sus vinculaciones. En el plano criminológico, muchos análisis de ARS vinculados con la centralidad dan cuenta de la importancia de la relación inversa entre grado nodal y centralidad de intermediación a la hora de detectar actores centrales en una red criminal que voluntariamente buscan esconder su rol protagónico. A decir de Miceli y otros,

> "La literatura sobre redes delictivas sostiene que las diferencias entre el grado nodal y la intermediación permiten iluminar patrones de posicionamiento estratégico capaces de reducir el riesgo de detección y mantener el control sobre las actividades delictivas al mismo tiempo. Sin embargo, la identificación de este patrón es compleja cuando las medidas aparecen como altamente correlacionadas." (Miceli et al., 2016:57)

De esta forma, la centralidad combinada es un índice que se obtiene de la división entre la centralidad de intermediación y la centralidad de grado. Este indicador busca resaltar aquellos nodos que tienen pocos vínculos pero de muy buena calidad, obteniendo de esta manera un posicionamiento estratégico dentro de la red[5].

3) La topología de la red y sus efectos en el diseño de intervenciones

Una vez analizados los nodos y los lazos de una red, una de las utilizaciones más concretas del ARS es el diseño de sus intervenciones por parte del sistema penal. El tema de las topologías de las redes, sus aspectos positivos y negativos fue estudiado exhaustivamente en los últimos años. Desde 1998 en adelante, con el descubrimiento de las llamadas redes libres de escala por parte de Barabási, Bonabeau, Jeong y Albert, se identificaron una serie de propiedades que impactan directamente en el diseño de intervenciones de redes. Según Reynoso, una red libre de escala:

[5] En próximos capítulos se mostrará una ejemplificación de este punto.

> "es extraordinariamente robusta: se puede destruir 80% de los nodos y el resto seguirá funcionando. Pero también es desproporcionadamente vulnerable a ataques selectivos: una eliminación de 5 a 10% de los hubs -que son poquísimos en relación con el tamaño de la red- alcanzaría para hacer colapsar el sistema o quebrar su unidad" (Reynoso, 2008:31).

Estos tipos de trabajos fueron el puntapié para investigar la resiliencia o vulnerabilidad de las redes criminales. En ese sentido, la literatura científica sobre el tema considera que, en primer lugar, no resulta tan efectivo intervenir los nodos de alta centralidad de grado como apuntar a los que tienen alto nivel de centralidad de intermediación. La supresión de estos últimos generan más disrupciones de la red (Xu y Chen, 2008; Calderoni, 2012).

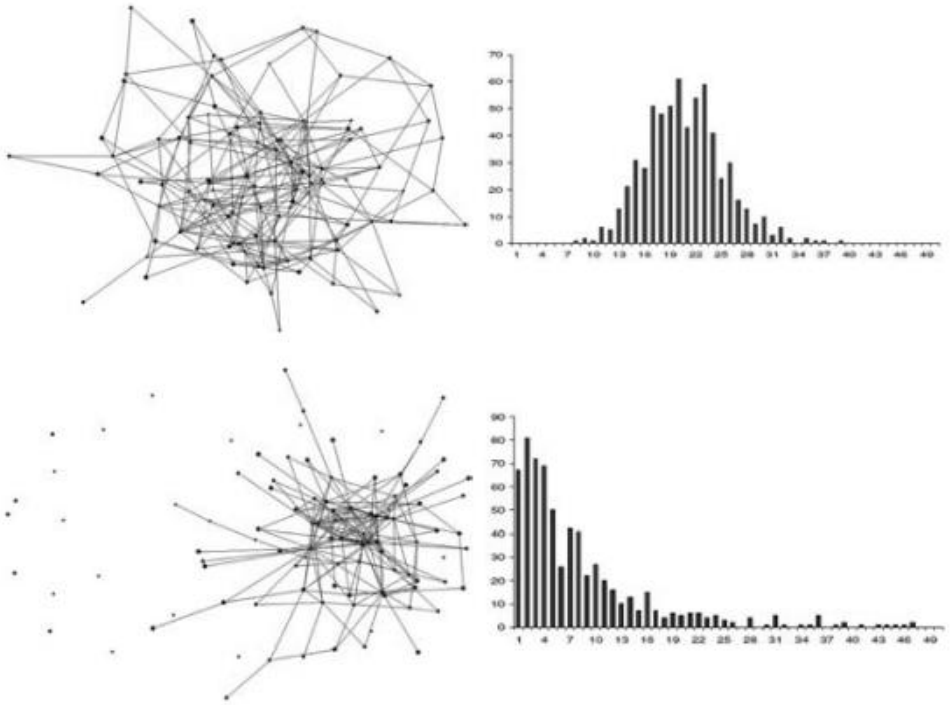


Figura 4 – En la parte superior se encuentra una red aleatoria y su correspondiente histograma. Del análisis del mismo se desprende que la relación entre cantidad de nodos y cantidad de relaciones sigue una distribución aproximadamente normal, es decir, todos los nodos tienen aproximadamente la misma cantidad de vínculos. En la parte inferior, por el contrario, se identifica una red libre de escala y su correspondiente distribución de ley de potencia en donde poquísimos nodos concentran la mayor cantidad de vínculos. (Reynoso, 2011: 192)

En segundo lugar, resulta interesante analizar el coeficiente de clusterización de las redes. Esta medida indica cuán conectados entre sí se encuentran los nodos. Un valor bajo indica

que la red no se encuentra muy conectada internamente mientras que, a la inversa, un valor alto indica una excelente conectividad de la red. En términos de una intervención, cuando se presenta un nivel bajo de coeficiente de clusterización, la remoción de nodos específicos podrían generar importantes quiebres en la red. Por el contrario, la supresión de un nodo en una red con alto nivel de coeficiente de clusterización no generaría una desconexión entre partes relevantes. Calderoni, al estudiar una organización narcotraficante italiana, afirma que:

> "...his pattern suggested that 'Ndrangheta groups may be particularly resilient to law enforcement intervention, since the removal of the most central nodes may be easily remedied through existing network connections, and the arrested individuals may be subsequently replaced with other participants." (Calderoni, 2012: 341)

Más allá de los mencionados aportes del ARS a la investigación penal, también hay que hacer explícita mención a sus limitaciones. En ese plano, la persona analista de redes tiene que tener plena consciencia de que los datos con los que cuenta al inicio de su desempeño profesional dependen inevitablemente de la hipótesis de investigación penal que guió la investigación y del desempeño de los actores judiciales y/o policiales al momento de la recolección de los mismos (Calderoni, 2012; Miceli et. al, 2016).

Las formas en las que intervienen dichos actores son muy relevantes. La definición de las entidades y sus vínculos como así también los datos recolectados generalmente no son elaborados por el analista de redes, sino que ya vienen prefigurados. Esto puede acarrear la presencia de sesgos en la investigación en los que el analista no puede tener mayor injerencia. En ese sentido, mucha de la calidad de la inteligencia criminal extraída del análisis va a depender del buen o mal desempeño de las personas involucradas en las anteriores instancias.

2.2.3 - El ARS y el análisis de telecomunicaciones

Si bien en el texto fundacional de Sparrow se comenta la aplicación del ARS al análisis de telecomunicaciones, lo cierto es que esa mención no se profundiza en desarrollos explícitos. Autores como Campana y Varese sostienen que "en los últimos años el análisis de redes

sociales ha sido ampliamente adoptado para el estudio de grupos criminales. Una fuente de datos relativamente descuidada son las conversaciones telefónicas interceptadas por la policía" (Campana y Varese, 2011: 27).

Esto no significa que el análisis de telecomunicaciones no haya sido abordado en alguna de sus características a través del ARS por parte de las fuerzas de seguridad e investigación penal, aunque sí se puede aventurar que dicho conocimiento no fue explicitado debidamente. Solo a partir de los últimos años es que han aparecido trabajos académicos específicos que dan cuenta sobre los procedimientos metodológicos y las problemáticas a resolver al momento de analizar telecomunicaciones.

El primero de dichos desarrollos abocados completamente a combinar el ARS con el análisis de telecomunicaciones es el trabajo de Catanese, Ferrara y Fiumana. Allí, los investigadores sostienen que el uso cada vez mayor de los teléfonos celulares en la vida cotidiana se refleja también en su adopción ilícita (coordinar actividades ilegales o comunicar decisiones son ejemplo de ello). Y que, para poder aprehenderlos, el ARS constituye una perspectiva fructífera aunque no exenta de dificultades:

> "The structure of criminal networks could be efficiently formalized by means of graphs, whose nodes represent actors of the criminal organizations (or, in our case, their mobile phones), and edges represent the connections among them (i.e., their phone communications). The graphical representation of data extracted from log files is a simple task, while its interpretation may result hard, when large volumes of data are involved" (Catanese et al, 2011: 15).

En dicho trabajo, los autores sostienen que a partir del tráfico de telecomunicaciones las fuerzas de seguridad y las agencias penales distinguen tres tipos de análisis: el relacional (en referencia a cómo se vinculan los abonados entre sí), el espacial (relacionado a la geolocalización de comunicaciones mediante el impacto en celdas telefónicas) y el temporal (utilizado para estudiar todas las variables dinámicas de las comunicaciones como ser fecha y hora o duración) (Catanese et al, 2011:2018).

A partir de allí presentan un software forense de desarrollo propio denominado "*LogAnalysis*". Los investigadores documentan las etapas necesarias para entrecruzar información de telecomunicaciones, como ser la importación de los datos, la normalización y limpieza de datos, la exploración de datos, el análisis de la información y su posterior visualización. Por último, presentan el desempeño del "*LogAnalysis*" aplicado a un caso real para ejemplificar la utilización de diversos estadísticos, filtros de datos, medidas de centralidad y algoritmos de visualización de grafos para obtener conocimiento útil a partir de la información de las comunicaciones telefónicas previamente estructurada (Catanese et al. 2011).

Otro artículo en donde se conjuga ARS y comunicaciones telefónicas es el realizado por Campana y Varese, que ya fue mencionado anteriormente. Allí los investigadores explicitan criterios y técnicas de análisis para abordar interceptaciones telefónicas. Entre los prerrequisitos para garantizar la rigurosidad de las conclusiones, los autores sostienen tres criterios: 1) que los usuarios de abonados intervenidos no intuyan que sus dispositivos están siendo escuchados; 2) que la cobertura del grupo criminal sea razonablemente amplia; y 3) que se encuentre disponible una muestra lo suficientemente grande para el análisis. Sin el cumplimiento de estos tres criterios cualquier tipo de análisis podría estar severamente sesgado (Campana y Varese, 2011).

En referencia a las técnicas de análisis de este tipo de información, el trabajo sostiene que el ARS permite mapear las conexiones, describir la fuerza de las relaciones entre actores y testear hipótesis del estilo quién es probable que esté conectado con quién en el futuro. También se pone énfasis en que el ARS puede ayudar a reconstruir la organización interna e informal de una red criminal en función de los patrones de conexiones de los actores. En ese sentido, los autores afirman que:

> "The internal structure uncovered by SNA is the informal one. In other words, we might know that a boss, an underboss and several team leaders exist in a group, but we are might have direct access to the boss, bypassing the formal hierarchy. Such a feature might predict future promotion, or conflict" (Campana y Varese, 2011: 25).

Por otra parte, se debe mencionar el interesante trabajo de Villedieu quién utilizó el concepto de red no sólo en términos de ARS sino también como modelo mismo de la base de datos (Villeedieu, 2015)[6]. Para ello confeccionó grafos a partir de listados de comunicaciones telefónicas y fue aplicando filtros temporales y espaciales a partir de la metadata de las comunicaciones. También consultó subgrafos de la red aplicando el criterio de mostrar los nodos que se encuentren a dos pasos de distancia. Con ello exploró distintas visualizaciones y a la vez logró jerarquizar datos específicos en medio de tanta información.

[6] Las denominadas bases de datos orientadas a grafos (bdog) representan una subvariante de las bases de datos no-sql. Las bases de datos que no siguen el modelo relacional cada vez son más utilizadas ya que se necesitan estructuras de datos menos rígidas o porque algunos tipos de consultas (sobre todo las que hacen hincapié en vínculos o conexiones) implican complejas operaciones a la vez que requieren mucha capacidad de cálculo. En términos técnicos, las bdog son eficientes ya que se pueden definir como un sistema que provee adyacencia sin consultar índice. Esto es lo que permite un mejor rendimiento para consultas que involucren relaciones: el costo es lineal a la cantidad de nodos adyacentes.

3 - Desarrollo y análisis del problema de investigación

Ahora bien, cabe realizar una pregunta central: si desde el artículo inaugural de Sparrow a comienzos de la década del 90 ya se tenía un programa de aplicación del ARS a la investigación penal y si se tienen en cuenta los importantes avances tecnológicos, de desarrollo de software y metodológicos alcanzados ¿por qué no se aplica de forma global y consistente esta perspectiva en la investigación penal?

Mi doble condición como científico social e investigador penal me permitió elaborar tres hipótesis sobre los motivos de esta cuestión. En primer lugar, considero que la utilización de software empaquetado para recolectar información, representarla en forma de red y analizarla funciona como una "caja negra" para las fuerzas de seguridad y los agentes judiciales. Los cursos y capacitaciones institucionales de los cuales pude participar están orientados más al marketing que a la explicación del funcionamiento de los programas. Tal es así que ante cualquier circunstancia inesperada (un requerimiento nuevo, una presentación distinta de los datos) la capacidad de innovar o replantear diseños reticulares es muy limitada. No existe software, por más funcionalidades que tenga, que pueda prever y abarcar todas las necesidades en investigación criminal, por lo cual resulta más útil saber utilizar unos cuántos ante cada situación. Al igual que un buen instrumento es necesario pero no hace a la excelencia del músico, ningún software reemplazará la indispensable mirada experta del analista de redes.

En segundo lugar, los softwares empaquetados de redes se llevan muy mal con la *"big data"*, específicamente con *"las tres V de big data"*, es decir, con el volumen, la velocidad y la variedad. Según el economista especializado en estadística y econometría Walter Sosa Escudero,

> "la primera de las V hace referencia a "big" -mucho-. La segunda se refiere a que los datos de big data se generan a una velocidad que los hace disponibles a una tasa prácticamente virtual, en tiempo real. Y la tercera -variedad- remite a la naturaleza espontánea, anárquica y amorfa del objeto que ahora llamamos 'dato'." (Sosa Escudero: 2019)

En mi experiencia laboral y en conversaciones con colegas converge la opinión de que los softwares empaquetados se "cuelgan" al intentar realizar procedimientos habituales como el preparado del dataset, el procesamiento de métricas o la visualización de redes cuando se enfrentan a cientos de miles de datos reticulares. En investigaciones penales "pequeñas" y "simples" se escala rápidamente a grandes volúmenes de datos. Cuando las causas son verdaderamente extensas, por ejemplo, hemos tenido la posibilidad de trabajar con más de tres millones de registros telefónicos.

Por último, mi tercera hipótesis sobre la falta de aplicación consistente del ARS en materia criminal es que en general las fuerzas de seguridad y los agentes judiciales no son formados en términos de analistas de redes. Dicha tarea es resultado de un proceso arduo en donde se deben aprender distintas formas de diseño de redes, técnicas de recolección de datos, algoritmos de análisis, formas de interpretación y visualización de las conclusiones. Las consideraciones epistemológicas, los núcleos teóricos, las diversas técnicas y metodologías como así también toda la parte algorítmica de métricas y visualizaciones no resulta algo de rápida asimilación. Es más, difícilmente constituya la expertise de un solo analista sino más bien de equipos interdisciplinarios que deben conformarse.

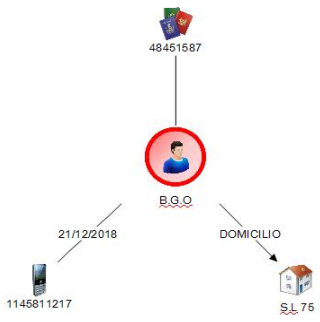
Tuve la oportunidad de acceder y revisar muchos informes de telecomunicaciones en donde se utilizaron modelos de redes que sirven para ejemplificar algunas de las hipótesis antes descriptas. En ese sentido, analizar un trabajo policial de entrecruzamiento de datos telefónicos arroja luz sobre sus límites tal como se lo está aplicando. El primer punto para mencionar hace referencia al desempeño de los programas empaquetados. En un informe técnico 2018 de una fuerza policial provincial se puede leer que:

> "Es dable destacar que debido al gran caudal de registros telefónicos proporcionados por la empresa de telefonía móvil [...], al realizarse el gráfico de entrecruzamiento por frecuencia y terceros en común, el sistema colapsa; NO pudiendo obtener resultado gráfico de entrecruzamiento".

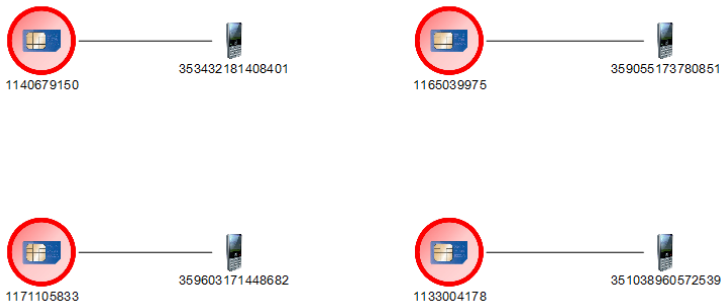
Esta oración del informe explicita las dificultades de los softwares empaquetados de entrecruzamiento al momento de tratar con grandes volúmenes de información. Pero, profundizando un poco la reflexión, el problema principal no es el tamaño de los datos de entrada, sino del tipo de operación que se le está requiriendo. El cálculo de "terceros en común" o la identificación de caminos de una red en términos computacionales no resulta nada trivial dada la explosión combinatoria.

Por otra parte, es importante tener presente que el aporte principal del ARS no es la posibilidad de realizar un gráfico de la red. La mayor parte de la inteligencia criminal que puede brindar el ARS no está relacionada con la parte visual sino con los indicadores de la información relacional de base. Es más, el entrecruzamiento de información de telecomunicaciones se podría expresar en redes pero también con otros recursos gráficos como pueden ser matrices o tablas. Sigue teniendo raigambre la noción del análisis de redes como *"herramienta pictórica"* que describiera críticamente Sparrow hace ya casi 30 años.

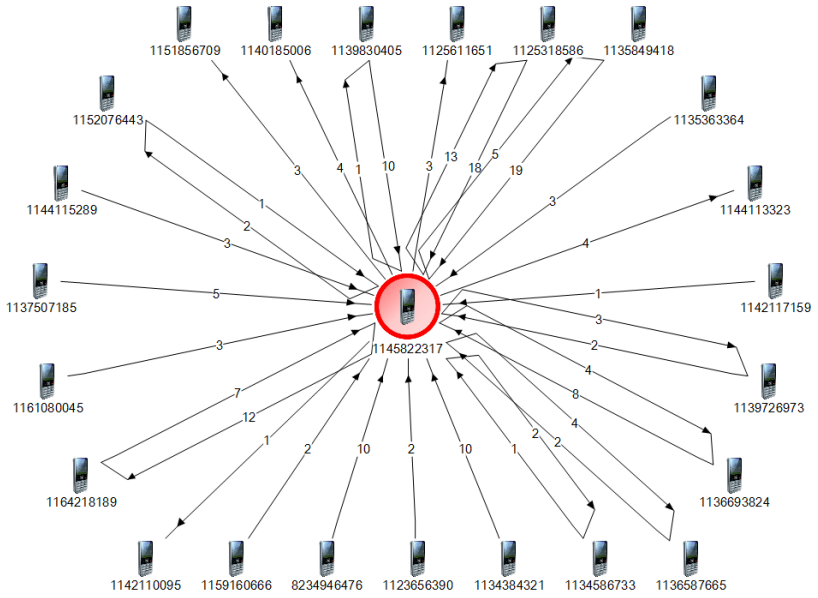
Un defecto encadenado al anterior es utilizar el ARS para mostrar algo que fácilmente podría haber sido expresado mediante otros recursos. Coincido con el antropólogo Carlos Reynoso al insistir en la necesidad de cuestionar "el hábito de reduplicar mediante las redes, su topología y sus álgebras concomitantes lo que ya sabemos o hemos aprendido a intuir por otros medios, lenguaje natural incluido" (Reynoso, 2009). Este tipo de error se evidencia en las siguientes redes:



A



B



C

Figura 5: A - Datos de titularidad de un abonado (número de abonado, fecha de alta, titular, DNI del titular, domicilio de facturación). B - Impactos de IMEI (abonados que traficaron comunicaciones en el dispositivo). C - Tráfico de SMSs de un abonado telefónico. Todos los datos fueron modificados del original para conservar el anonimato.

Las tres redes de la figura precedente dan cuenta de que es importante no caer en el fetiche de la graficación cuando los mismos datos no lo ameritan. Según Reynoso, es central

> "buscar soluciones reticulares (o de la naturaleza formal que fuere) en función de los recursos lógicos o algorítmicos que dicho planteo está en condiciones de aportar y no tanto en función de un grafismo que se obstina en replicar en el registro visual (en aras de un presunto esclarecimiento) lo que consideramos observable o lo que creemos saber desde siempre merced a la palabra". (Reynoso, 2009)

En ese sentido, las redes A y B podrían tranquilamente ser expresadas de forma más clara mediante lenguaje natural. Respecto a la red C uno puede darse cuenta de forma previa de su topología de estrella observando los datos. Más eficiente en el análisis de la información hubiera sido presentarlos mediante una tabla que contenga al abonado de interés, sus

interlocutores y la cantidad de comunicaciones cursadas entre ambos. En ninguno de los tres casos se justifica utilizar el modelo reticular.

Desde ya que no cuento con una visión completa y exhaustiva sobre la realidad de todas las instituciones que se desempeñan en ámbitos de investigación penal a nivel nacional, regional e internacional. Estas hipótesis no tuvieron un desarrollo sistemático ni alcanzaron un nivel de generalización más allá de mi acotada experiencia profesional. Igual de cierto es que existen muy pocos estudios en la literatura científica de la aplicación del ARS en entornos operativos como el de las fuerzas policiales o las oficinas judiciales debido a las entendibles dificultades de acceso al campo por cuestiones de seguridad (Duijin y Klerks, 2014; Burcher y Whelan, 2017).

A pesar de la poca producción académica, los trabajos existentes coinciden con las problemáticas que identifiqué en mi experiencia profesional. Autores como Miceli, Orsi y Rodríguez García lo describen específicamente:

> "la aplicación del ARS en el terreno penal se encontró asociado a sus insumos regulares: la focalización de casos de baja intensidad y complejidad derivó así, a la larga, en un uso mecánico de la herramienta. Un aspecto cuestionable de este proceso de mecanización es el deficiente empleo de las prestaciones de análisis, incluso si, en los casos en los que se han generado soluciones informáticas que vinculan distintos tipos de criminalidad y ARS, se las compara con paquetes de *software* como UCINET, Gephi, Visone u ORA." (Miceli et. al, 2016:133)

Por otra parte, y a miles de kilómetros de distancia, Burcher y Whelan, en su investigación con fuerzas policiales de Australia, sostienen que las dificultades en el procesamiento de grandes volúmenes de información constituyen un asunto urgente:

> "As put by one analyst, 'you are constrained by the power of the software, I've nearly broken Analyst Notebook, I did ring them up and ask, how much [data] can I actually put in?' This would suggest that intelligence analyst may be significantly inhibited in their ability to use SNA by the choice if which analytical tools are made available to them. Furthermore, the issue of large datasets, or what is

> commonly referred to as data or information overload, is a challenge that has only gotten worse for law enforcement." (Burcher y Whelan, 2017: 9)

También llegaron a conclusiones similares sobre la necesidad de brindar más formación en análisis que en enfatizar la idea de que la solución se obtiene por el lado del desarrollo de software únicamente. A partir de su investigación de campo, estos autores sostienen que:

> "To reinforce the point that training in appropriate software and SNA techniques is essential, one analyst emphasises that 'throwing more human resources into things isn't necessarily the answer', and that 'skilling them up and giving them the tools that they actually require and understanding some of the concepts' will decrease the 'disconnect between the theory that's out there and actually how we might use it'." (Burcher y Whelan, 2017: 13)

Ante estas limitaciones en la aplicación del ARS al tratamiento de las telecomunicaciones en entornos operativos de investigación penal es que creo conveniente documentar los procesos de trabajo que hemos logrado estandarizar. Llevar a cabo esto implica explicitar los procedimientos y metodologías que desplegamos en los distintos pasos del ciclo de inteligencia criminal en el análisis de comunicaciones telefónicas. El primero de esos pasos es el de la recolección de los datos en donde revisaremos las distintas fuentes con las que se puede nutrir la investigación penal. En segundo lugar, hace referencia al procesamiento de la información, en donde explicaremos conceptualmente las reglas utilizadas para preparar los datos y para generar las tablas con distintas vistas sobre los registros telefónicos. Por último, en la parte de análisis y producción (donde la información se convierte en inteligencia) aplicaremos el ARS como enfoque heurístico.

3.1 - Recolección de datos sobre telecomunicaciones

Lo primero que hay que llevar a cabo antes de identificar las fuentes de información disponibles es describir los tipos de datos que existen en cualquier comunicación. En ese sentido y tal como se observa en la Figura 6, las comunicaciones presentan dos grandes tipos de datos: por un lado el *contenido* o el mensaje objeto de comunicación entre dos o más interlocutores y, por el otro, los *metadatos* que refieren al contexto desde el cual se desarrolló una comunicación. Dichos metadatos o información asociada a la comunicación son: abonados interlocutores, titularidad de los abonados, domicilio de facturación de los abonados, sentido de la comunicación, tiempo (fecha y hora) y ubicación (identificador de celda, dirección, latitud, longitud y localidad).

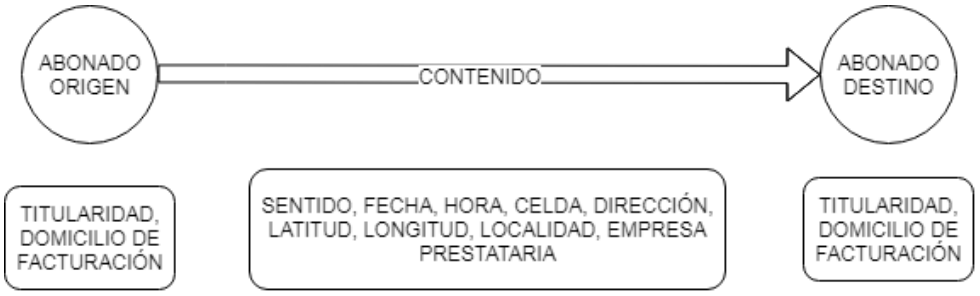


Figura 6 – Estructura conceptual de una comunicación telefónica y sus correspondientes tipos de datos (esquema de elaboración propia).

Se trate de un caso chico o uno de gran envergadura, cuando analicemos telecomunicaciones siempre encontraremos esos tipos de datos. Ellos son los necesarios para llevar adelante los cruces de información. Sin embargo, la presencia de los mismos puede variar en su manifestación dependiendo del origen. Es por ello que a continuación nos vamos a detener brevemente en las tres fuentes principales de recolección de información sobre telecomunicaciones: las interceptaciones telefónicas, las extracciones forenses de celulares y la solicitud de datos a las prestatarias.

La primera fuente de recolección de datos es la de interceptaciones telefónicas. En Argentina, la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado (DaJuDeCO)

dependiente de la Corte Suprema de Justicia de la Nación es la única dependencia estatal autorizada para realizar escuchas telefónicas legales. Cuando en una causa se ordena realizar interceptaciones a determinados abonados de interés, los datos son incorporados a los expedientes judiciales mediante soportes ópticos.

La ventaja de este método de recolección es que se obtiene el acceso al contenido de las comunicaciones (incluso en tiempo real si así es requerido) y el formato, al originarse en una única dependencia, es estandarizado. Las desventajas que presenta es que en numerosas ocasiones se registran faltantes de información (sobre todos los vinculados con los impactos de celdas telefónicas), resulta costoso en tiempo y recursos humanos realizar un análisis de todo el contenido de los mensajes y, por último, aún existe un atraso del marco regulatorio estatal y tecnológico de las prestatarias para poder interceptar tráfico de datos (comunicaciones entre diferentes aplicaciones del celular como por ejemplo WhatsApp).

La segunda fuente de recolección de datos de telecomunicaciones proviene de las extracciones forenses de dispositivos celulares. Las empresas del rubro se dedican al diseño del hardware y software necesarios para superar las medidas de seguridad de los dispositivos celulares y los sistemas operativos con el objetivo de acceder a la información almacenada en las memorias. La compañía mundialmente más conocida es Cellebrite y su producto se denomina UFED (Universal Forensic Extraction Device). Con estos tipos de sistemas el máximo nivel de información recolectada proviene de una extracción de tipo física ya que es la única que realiza una copia "bit a bit" de la memoria interna del dispositivo móvil. En otras palabras, este tipo de operación permite extraer información tanto de los archivos ya existentes como del espacio no localizado y no asignado (lo que significa la posibilidad de acceder a información "borrada" por el usuario). Si bien este tipo de extracción es la más completa que se puede realizar, las medidas de seguridad de las empresas productoras de dispositivos celulares no pocas veces obligan a utilizar otro tipo de extracciones con un menor nivel de profundidad.

Las ventajas de las extracciones forenses están relacionadas con la posibilidad de acceder al contenido de las comunicaciones e, incluso, del contenido borrado por el usuario. Por otra parte, el formato de salida de las extracciones forenses está estandarizado. Las desventajas respecto al contenido son las mismas que con la interceptación de comunicaciones

telefónicas, es decir, se requieren mucha inversión de tiempo y recursos humanos para analizar con profundidad todo el material. Otra desventaja es que, como cualquier dispositivo electrónico, existe una posibilidad de adulteración de datos aunque se requieren altos niveles de formación, experiencia y sofisticación para llevarlo a cabo. Por último, existe una tercera desventaja y es que no a todos los dispositivos celulares se les puede realizar una extracción de tipo física.

La tercera fuente de recolección es la información asociada brindada por las empresas prestatarias de servicios de telecomunicación. A ellas se les puede requerir información desde diferentes puntos de partida: 1) tráfico a partir de abonado, cuándo se le brinda a la prestataria determinados abonados de interés para la investigación en curso y ésta devuelve los registros de comunicaciones entrantes y salientes correspondientes; 2) tráfico a partir de celda, cuando se le brinda determinada zona de interés y la prestataria devuelve los registros de comunicaciones entrantes y salientes de aquellas antenas aledañas; 3) tráfico de IMEI, cuándo se le brinda la numeración unívoca de un dispositivo a la prestataria y ésta indica cuáles abonados (tarjetas SIM) impactaron en el dispositivo en cuestión.

La ventaja de solicitar datos a las prestatarias es que resulta muy raro que falte información. A su vez, la probabilidad de adulteración de los datos es muy baja. La principal desventaja de este procedimiento lo constituyen las importantes demoras y dificultades de gestión ante ellas. En segundo lugar, no hay un formato unificado de respuesta y cada prestataria presenta los datos de una forma distinta e incluso una misma puede hacerlo en más de un formato. Por otra parte, los tipos y duración de los datos resguardados por las empresas están pensados para el mundo comercial y no para la investigación penal. El déficit de regulación estatal sobre el área requeriría mayor atención. Como se dijo anteriormente, aún no existe la tecnología necesaria para obtener la información asociada a las telecomunicaciones con tráfico de datos.

3.2 - Preparación y procesamiento de datos

La herramienta que utilizamos para las diferentes tareas de preparación y procesamiento de los datos es una base de datos relacional. Sin entrar en detalles técnicos que no hacen al presente trabajo, hay que tener en cuenta conceptualmente que volcamos todos los registros de información telefónica en una base datos y que, desde allí diseñamos diferentes consultas en lenguaje SQL que logramos estandarizar a todos los casos para llevar adelante las reglas de transformación de datos y de generación de listados. Como veremos más adelante, a partir de dichos listados es que aplicaremos el ARS.

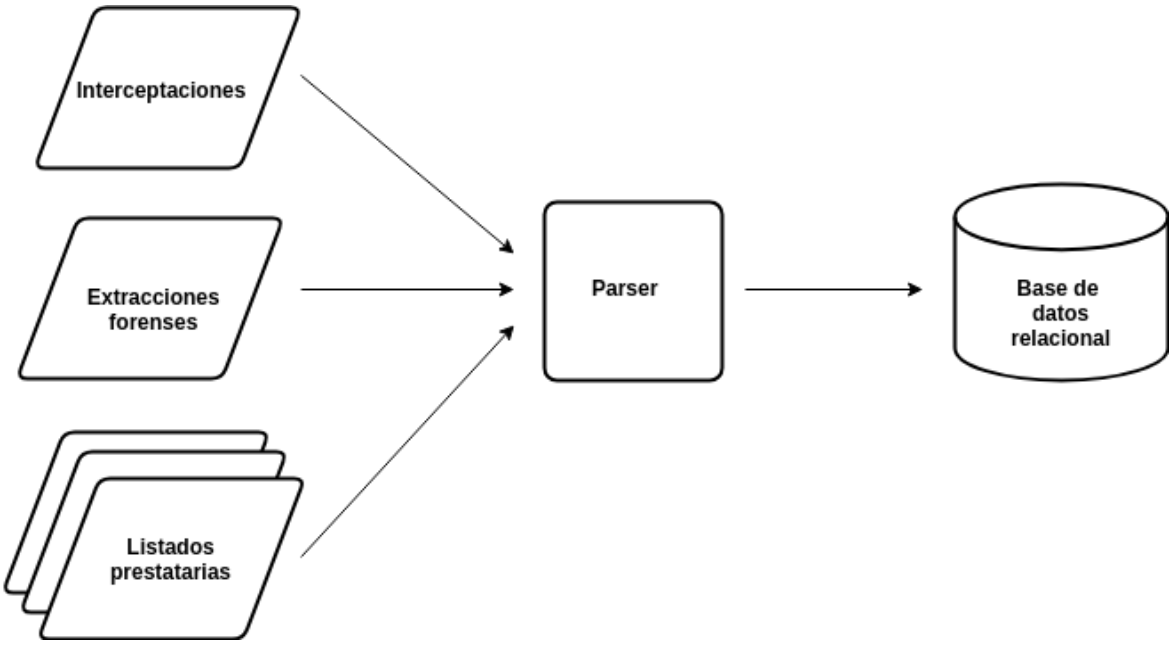


Figura 7 - Tipos de fuentes de datos de telecomunicaciones. Todas ellas son transformadas mediante diversas parsers para poder ser incorporadas y almacenadas en una base de datos relacional (esquema de elaboración propia).

Lo primero que hay que tener en cuenta es la normalización de los datos, es decir, la realización de distintas modificaciones necesarias para preparar los datos que van a ser procesados y analizados posteriormente. Esta etapa de preprocesamiento de los datos está compuesta por tres momentos: la estandarización de los abonados interlocutores implicados

en las comunicaciones, la eliminación de registros duplicados y la eliminación de abonados excluidos.

Las reglas para la estandarización de los abonados tienen el objetivo de transformar los registros para que se adecuen a la norma estipulada por el Plan Fundamental de Numeración Nacional estipulados por el ENACOM (Ente Nacional de Comunicaciones). En ese sentido, si bien en Argentina para realizar una llamada telefónica es necesario marcar diez dígitos, lo cierto es que las empresas prestatarias de servicios de telefonía registran los abonados algunas veces con más y otra con menos dígitos que los indicados por el Plan Fundamental. Por ejemplo, el abonado nro. "*11-1111-1111"* podría estar registrado como "*54-9-11-1111-1111"* o quizá "*15-1111-1111"* dependiendo del criterio de la compañía. Esto podría generar que un mismo número que estuviera registrado de forma diferente por dos compañías distintas, o incluso por una misma compañía, sea almacenado en la base de datos como si fueran dos abonados distintos.

A los fines de evitar tal resultado, y con el objeto de contar con datos consolidados, en los casos en que fue posible se procedió a modificar los elementos accesorios a las líneas telefónicas (por ejemplo, el caso del *"0"* en código de área *"011"* correspondiente al Área Metropolitana de Buenos Aires). Por consiguiente, los abonados fueron registrados como *"11-1111-1111"*, manteniendo sus respectivas características de áreas y el resto de los dígitos que identifican la línea particular.

Hasta la fecha, el equipo al cual pertenezco aplica las siguientes reglas de transformación de los datos originales:

1. Si un abonado tiene más de diez (10) dígitos y empieza con *"0"*, se sustrae éste.
2. Si tiene doce (12) dígitos y empieza con *"11-15"*, se elimina el *"15"*.
3. Si tiene diez (10) dígitos y empieza con *"15"*, éste se reemplaza con *"11"*.
4. Si tiene doce (12) dígitos y empieza con *"54-11"*, se extrae el *"54"*.
5. Si tiene trece (13) dígitos y empieza con *"54-9"*, se extirpa dicha numeración.
6. Si tiene ocho (8) dígitos y empieza con *"2"*, *"3"*, *"4"*, *"5"*, *"6"* o *"7"*, se le agrega el prefijo *"11"*.

7. Si comienza con *"A"* se suprime dicho carácter.

Desde ya que la información agregada o suprimida a cada abonado no altera su identidad o titularidad, toda vez que se trata de información accesoria utilizada exclusivamente a los fines de llevar a cabo un correcto cruce de información. También hay que destacar que en los casos que los abonados tengan siete (7) dígitos o menos[7], en los que posean trece (13) -sin comenzar con *"54-9"*- o no encuadren en ninguno de los puntos detallados precedentemente, no se ha podido normalizar la información por lo que se mantuvieron los datos como fueran registrados por las respectivas empresas telefónicas.

La segunda tarea en la normalización de los datos refiere a la eliminación de los registros telefónicos duplicados. Esto se debe a que en numerosos casos los lotes de información que provienen de múltiples fuentes hacen referencia a una misma comunicación real. Cabe resaltar que en términos de la base de datos no se trata de una eliminación sino más bien en la marcación de un registro como duplicado. Esto se debe a que en realidad, al momento de la valoración de un registro comunicaciones, puede ser de utilidad evaluar su fiabilidad menor o mayor dependiendo del tipo de fuente de registro o su concordancia en múltiples fuentes.

Por último, no toda comunicación registrada es relevante para una investigación penal. Se debe recordar que mucho de lo registrado no corresponde a un sistema creado para la investigación penal sino para los usos comerciales de las empresas prestatarias de servicios de comunicación. En ese sentido, prácticamente en todos los casos se registran abonados telefónicos que no cumplen con las reglas básicas de numeración de la Argentina (ENACOM) por lo cual no conviene tenerlos en cuenta (mas nunca borrarlos)[8]. Acá hay un

[7] En algunas ocasiones las empresas prestatarias de servicios registran abonados con 7 dígitos, omitiendo registrar el código de área.

[8] Ejemplos de abonados excluidos son: (vacio), *111, *124, *150, 151, *152, *2447, *25225, *25283, *2582, *2747, *2828, *444, *555, *611, *66266, *7526, *767, *9009, 0000000000, 0, 0000, 1, 3, 007, 008, 0010, 0012, 0013, 0015, 54, 110, 111, 112, 113, 114, 123, 130, 142, 144, 147, 150, 151, 152, 205, 210, 216, 222, 242, 246, 250, 252, 253, 262, 263, 321, 325, 333, 336, 345, 365, 424, 43A1D0, 444, 456, 505, 515, 554, 555, 582, 611, 622, 666, 732, 748, 767, 772, 773, 810, 811, 813, 955, 965, 999, 1010, 1122, 1221, 1515, 1533, 1611, 1616, 2016, 2020, 2045, 2090, 2112, 2233, 2244, 2282, 2323, 2345, 2347, 2365, 2442, 2582, 2633, 2747, 3050, 3131, 3132, 3372, 3388, 3456, 3579, 3733, 4021, 4141, 4445, 5437, 8520, 8830, 9357, 9428, 9988, 11011, 13013, 20161, 20200, 30500, 89338, 90400, 93590, 99910, 99913, 113311, 393766, 742671, 772676, 779988, 5411555, 99991100, 99991102, 99991103, 8009997424, 8009997700, 8009999699, 8223336633,

debate entre la fidelidad al registro de la comunicación o la búsqueda de cierta inteligencia criminal para eliminar el ruido que representan comunicaciones registradas pero no reales. Nuestra decisión ante esa disyuntiva es establecer un listado de "abonados excluidos" los cuáles no se tendrán en cuenta al momento de realizar el cruce de información.

Una vez terminadas las tareas de normalización de los datos pasamos a la etapa del procesamiento de la información propiamente dicho. Para ello es necesario, primero, tener en cuenta algunos parámetros informativos adicionales. Uno indispensable es la especificación de cuáles son los abonados observados. Los abonados observados, para nosotros, son aquellos de los cuales se nos brinda información de cualquier tipo de fuente o resultan de interés para la investigación penal. Todos los análisis que se realizarán están en función directa de los abonados observados. Otros dos parámetros optativos son las especificaciones temporales y espaciales potencialmente relevantes para una investigación penal.

Luego de definidos los parámetros de entrada, aplicamos distintas consultas generadas mediante SQL de forma estándar para cada caso. Dichas consultas generan como salida diferentes tablas que representan distintas vistas relativas a los datos y que se describirán a continuación.

8227773333, 8227776543, 9BC5E0, B111, B15, B150, B150B, B151, ClaroAviso, ClaroFE, ClaroHoy, D2BC7EF67789D, MOVISTAR, Movistar+, Restringido, S/D, WAP3, WEB.

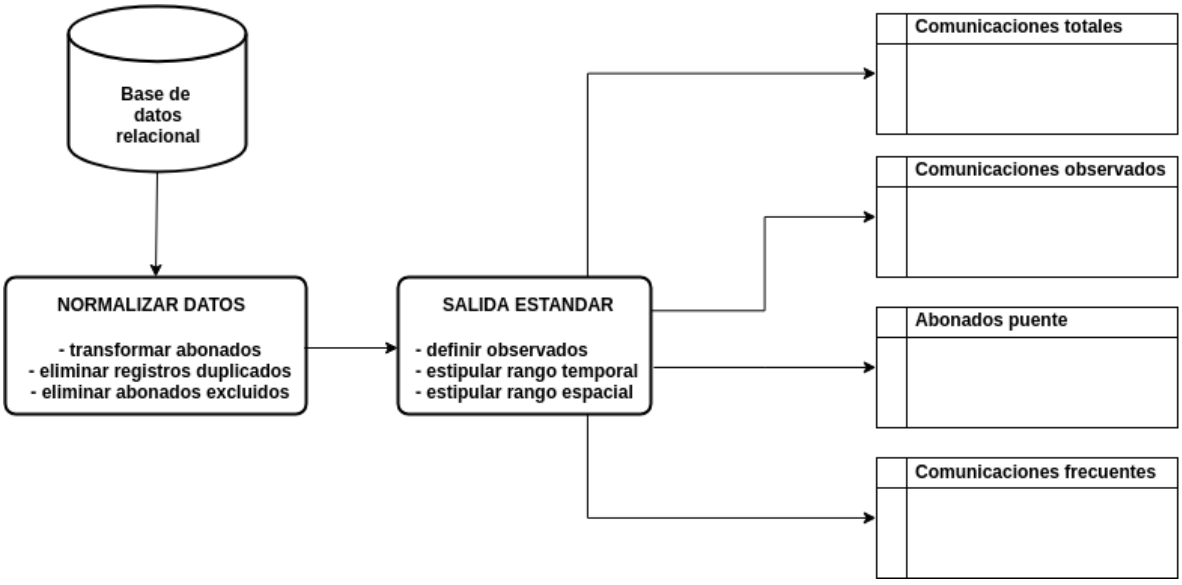


Figura 8 – Tareas para normalizar datos y parámetros necesarios para obtener una salida estándar de tablas (esquema de elaboración propia)

1 – Tabla de comunicaciones totales

Esta tabla contiene el listado completo de las comunicaciones normalizadas y consolidadas. La razón principal por la cual se estableció este producto como salida estandarizada es la facilidad que genera para el operador policial o judicial el tener en un solo archivo toda la información que antes se encontraba desperdigada en múltiples fuentes y formatos. En esta tabla se puede acceder a la totalidad de la información asociada o metadatos de las comunicaciones, como ser:

- interlocutor 1: el primer abonado que participa de la comunicación;
- titular 1: titularidad informada por las prestatarias o usuario asumido por los investigadores correspondiente al interlocutor 1;
- interlocutor 2: el segundo abonado que participa de la comunicación;

- titular 2: titularidad informada por las prestatarias o usuario asumido por los investigadores correspondiente al interlocutor 2;
- observado: permite identificar rápidamente cuál de los dos abonados interlocutores es de interés para la investigación;
- fecha: en qué día, mes y año se realizó la comunicación;
- hora: en qué hora, minuto y segundo se realizó la comunicación;
- duración: tiempo total de la comunicación, expresado en segundos;
- sentido: dirección en la que se realiza una llamada. Cuando es entrante se simboliza con una "E", con una "S" si es una llamada saliente y con una "T" cuando es saliente pero atiende el contestador automático;
- celda: código de identificación de la celda provisto por la prestataria por la cual traficó la comunicación
- dirección de celda: descripción de la calle donde está ubicada la celda provista por la prestataria
- coordenadas: latitud y longitud geográfica donde está ubicada la celda
- lote: identifica el nombre del archivo original de donde se extrajo la información;
- empresa: prestataria o fuente de pertenencia del archivo.

Hay dos cuestiones importantes a tener en cuenta. La primera es que la variable "lote" indica el origen del registro de la comunicación, es decir, de qué archivo fuente se extrajo la información. Esto garantiza la trazabilidad de los procedimientos realizados como así también resulta útil para localizar de forma ágil las fuentes de información desde la cual se sustentan los datos. La segunda cuestión a tener en cuenta es que el resto de las tablas que se van a presentar conceptualmente constituyen distintos subconjuntos de ésta tabla más general. Aquí va cobrando fuerza la idea de producir inteligencia ya que no se incorporan nuevos datos o información, sino que se los procesa de forma tal que generan conocimiento.

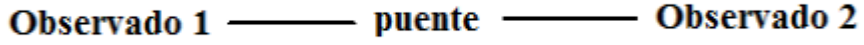
2 – Tabla de cruce de comunicaciones de observados

La segunda tabla de salida estándar es la de cruce de comunicaciones de abonados observados. Allí se encontrará un listado con las llamadas y los mensajes de texto que mantuvieron los abonados observados entre sí. Las variables de esta tabla son las siguientes:

- observado 1: el primer abonado observado que participa de la comunicación;
- observado 2: el segundo abonado observado que participa en la comunicación;
- fecha: en qué día, mes y año se realizó la comunicación;
- hora: en qué hora, minuto y segundo se realizó la comunicación;
- duración: tiempo total de la comunicación, expresado en segundos;
- sentido: dirección en la que se realiza una llamada. Cuando es entrante se simboliza con una “E”, con una “S” si es una llamada saliente y con una “T” cuando es saliente pero atiende el contestador automático;
- lote: identifica el nombre del archivo original de donde se extrajo la información;
- empresa: prestataria o fuente de pertenencia del archivo.

3 – Tabla de abonados puente

En esta tabla se evidencian cuáles fueron los abonados no observados que funcionan como “puente” entre dos abonados observados. Denominamos “puente” a aquella línea telefónica que se comunica con al menos dos abonados observados tal como se puede ver en el siguiente diagrama:



En las tablas confeccionadas nosotros incluimos los siguientes campos:

- observado 1: primer abonado observado con el que se comunicó el abonado no observado puente;
- 1-NO: cantidad de comunicaciones entre el abonado observado 1 y el abonado no observado puente;
- Abonado puente: número telefónico del abonado no observado puente identificado;
- NO-2: cantidad de comunicaciones entre el abonado no observado puente y el abonado observado 2;
- observado 2: segundo abonado observado con el que se comunicó el abonado no observado puente;
- total: suma de comunicaciones mantenidas entre los dos abonados observados y el abonado no observado puente;
- cantidad observados: suma de abonados observados con los que se comunicó el abonado no observado puente;
- descripción observados: números de los abonados observados con los cuales se comunicó el abonado no observado puente.

5 – Tabla de frecuencias de comunicaciones

En esta tabla se listan todas las díadas de abonados y se ponderan la cantidad de comunicaciones que mantuvieron. Otra posibilidad de ponderación es por duración total para cada par de interlocutores y no ya por cantidad de comunicaciones. Los campos de la tabla son los siguientes:

- observado 1: el primer abonado observado que participa de la comunicación;

- observado 2: el segundo abonado observado que participa en la comunicación;
- cantidad: frecuencia de comunicaciones entre cada par de observados;
- fecha y hora comienzo: comienzo de la primera comunicación entre los pares de abonados observados;
- fecha y hora fin: comienzo de la última comunicación entre los pares de abonados observados.

3.3 - Análisis de redes sociales (ARS) de comunicaciones telefónicas

Objetivo

El siguiente paso luego de la recolección y el procesamiento de los datos es el del análisis. Aquí es cuando entra la metodología de construcción de redes del ARS. Esta perspectiva permite de forma sistemática el análisis y la visualización de las tablas procesadas en el punto anterior utilizando las redes.

Como vimos anteriormente, una red es un modelo abstracto conformado por dos tipos de entidades: los "nodos" vinculados mediante "lazos". Teniendo los recaudos metodológicos correspondientes, podemos definir los nodos y los lazos de modo sustantivo según las particularidades de cada caso, en esta instancia atendiendo a las características de las comunicaciones entre abonados telefónicos. Esta forma de trabajo nos va a permitir:

1) analizar los nodos centrales o más relevantes de la red
2) identificar los lazos más fuertes o indispensables para la conectividad de la red
3) describir la estructura global de la red

Definición de díada

Lo primero que hay que explicitar es la definición de la unidad mínima de la red: la díada. En el ámbito donde trabajo, generalmente la díada la definimos de la siguiente forma:

Nodo	Vinculo	Nodo
Abonado observado	Lazo bidireccional y ponderado por frecuencia de comunicaciones	Abonado no observado

Figura 9 – Modelo de díada que constituye la unidad mínima de la red (esquema de elaboración propia).

Como se puede observar, para conformar las redes su unidad mínima está compuesta por un nodo de color verde que representa a un abonado observado, por otro nodo de color violeta que representa a un abonado no observado y un lazo de color negro que indica la presencia de una comunicación entre esos dos nodos. Para nuestro estándar, definimos que las comunicaciones sean modeladas como lazos no orientados para tener una interpretación más simple y eficaz de transmitir de los algoritmos de ARS que utilizaremos más adelante. Por otra parte, ponderamos los lazos de comunicaciones por la frecuencia de las mismas.

Desde ya que este es *nuestro* modelo, *nuestras* definiciones y *nuestras* asunciones. Existen muchas otras formas de representar una comunicación: por ejemplo los lazos pueden ser orientados (aportando más información sobre qué abonado origina una comunicación y qué interlocutor la recibe); o los lazos podrían ser ponderados por duración total más que por frecuencia. En nuestra experiencia, este modelo nos resulta óptimo, transformándose en un estándar para nuestro sistema. Sin embargo, tenemos la conciencia de que un caso especial o un requerimiento específico podría demandar modificaciones en la forma de modelar las redes.

Por otra parte, según nuestra definición de díadas, entendemos que proyectando el modelo de red se pueden describir tipos de nodos distintos:

- nodos o abonados observados: generalmente son los originantes de la información y pueden provenir de varias fuentes o de una sumatoria de las mismas.
- nodos o abonados no observados: son todos aquellos abonados interlocutores de los abonados observados. Por su posición estructural, pueden presentar dos características.
    - nodos o abonados no observados puente: son todos aquellos abonados no observados que se comunican con dos o más nodos abonados observados.
    - nodos o abonados no observados referidos: son todos aquellos que no cumplen con la función de puente, es decir, aquellos nodos abonados no observados que solo se comunican con un abonado observado.

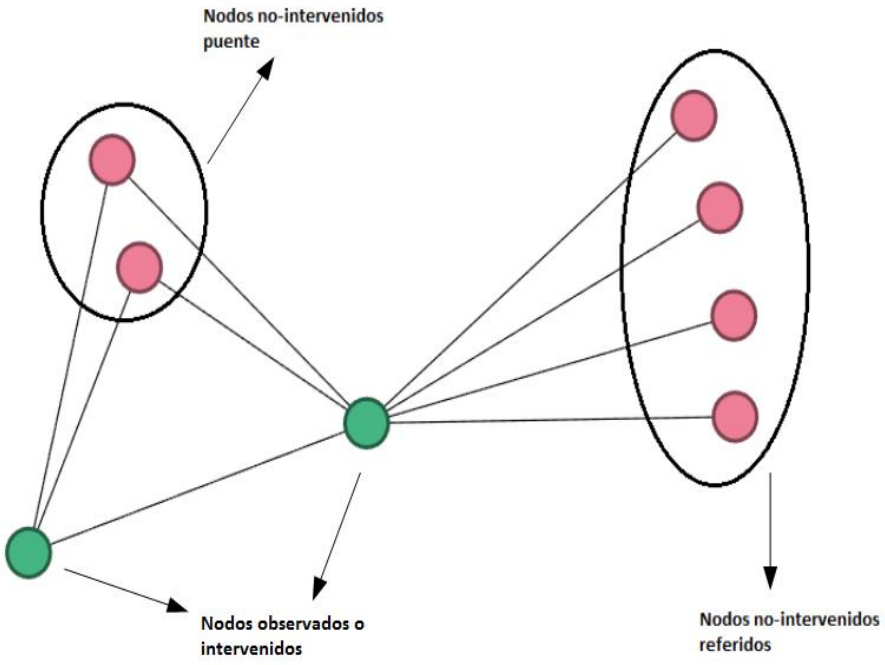


Figura 10 – Modelo de comunicaciones para nodos observados, no observados puente y no observados referidos (esquema de elaboración propia).

Pasajes de tablas a redes

Las tablas que componen la salida estándar para cada investigación penal no son otra cosa que matrices de incidencia, por lo cual pueden ser representadas en forma de red. En ese sentido, cada tabla tiene su red asociada:

Tabla	Red	Descripción
Comunicaciones totales	Red total	Contiene todas las comunicaciones entre abonados observados, puente y referidos
Cruce observados	Red observados	Contiene las comunicaciones entre abonados observados
Abonados puente	Red núcleo	Contiene las comunicaciones entre abonados observados y con los puentes
Abonados frecuentes	Red de comunicaciones frecuentes	Contiene las comunicaciones que superan un umbral para ser considerado frecuente en donde aparecen observados, referidos y quizás puentes

Tabla 1 – Resumen de tablas, su equivalente en red y su descripción (esquema de elaboración propia).

Para ejemplificar los conceptos vamos a presentar el análisis de un caso real[9]. El mismo consistió en una solicitud de colaboración a nuestra oficina para analizar el flujo de comunicaciones de una asociación criminal acusada de suprimir el estado civil de un menor. El objetivo general que se nos comunicó era doble: en primer lugar debíamos analizar las comunicaciones entre los abonados observados para generar la prueba de que se trataba de una organización consolidada; en segundo lugar, nos solicitaban detectar nuevos abonados no observados que sean de potencial interés para la investigación en curso.

Para ello la fiscalía nos aportó la información asociada de las telecomunicaciones correspondientes a 26 abonados observados en un rango temporal de dos meses. Dicha información constituyó un total de 20 lotes de información (archivos) de prestatarias de servicios telefónicos en las que se registraron 22.745 comunicaciones.

[9] Desde ya que todos los nombres, abonados y referencias fueron transformadas para garantizar el anonimato de las personas involucradas en el hecho investigado.

Red Total

Luego de realizadas las tareas de preprocesamiento (carga) y procesamiento (normalización) se generaron las distintas tablas. La primera de ellas es la tabla de Comunicaciones Totales en donde, como vimos, se encuentra todos los registros de comunicaciones normalizados, es decir, 22.265 comunicaciones. La representación gráfica de la tabla en cuestión es la siguiente:

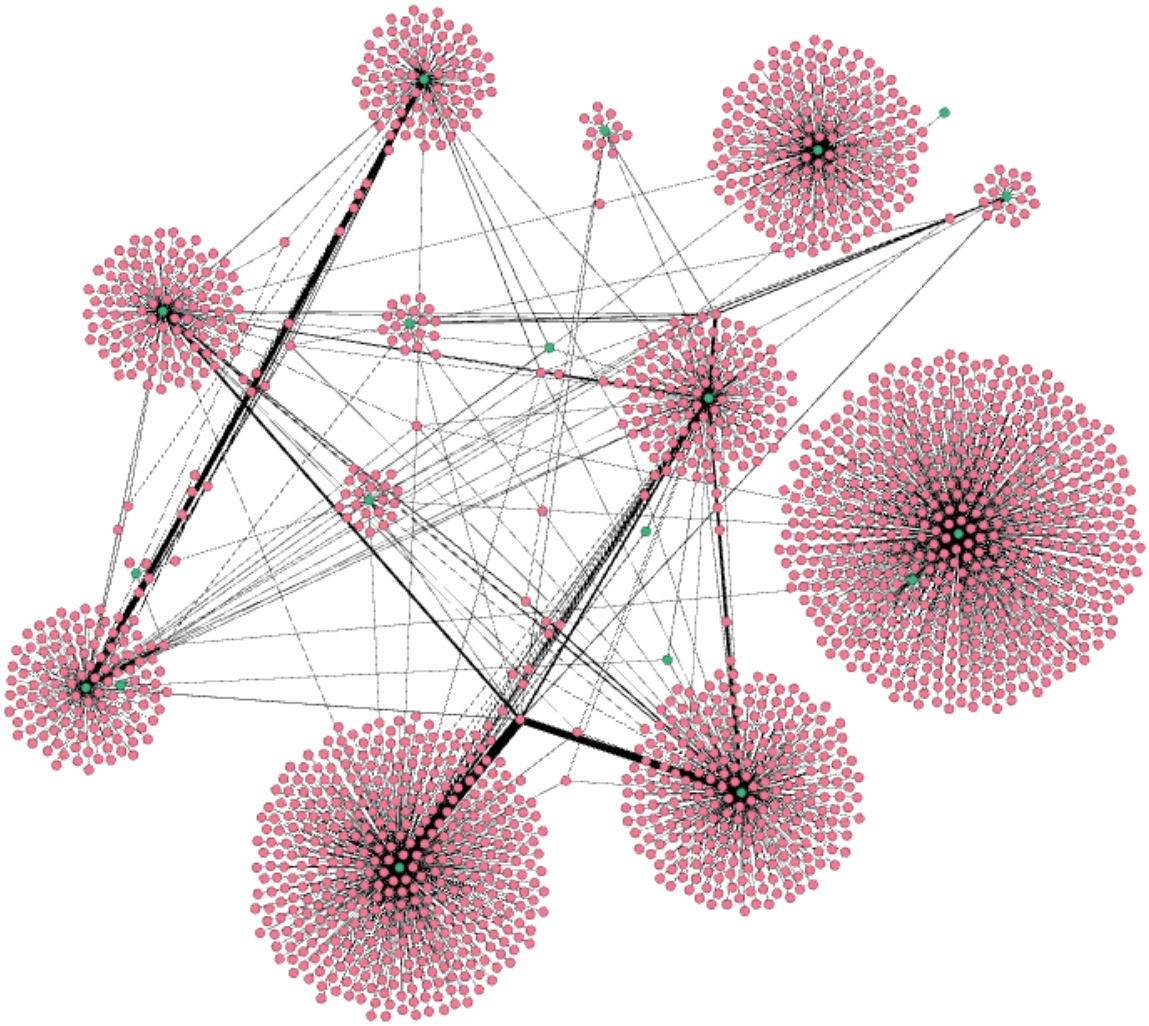


Figura 11 – Grafo de la Red Total (esquema de elaboración propia con el software Gephi 0.9.2).

El grafo contiene 2094 nodos y 2216 vínculos. Lo primero que se puede afirmar es que la red total contiene un solo componente, es decir, todos los abonados telefónicos están conectados entre sí, ya sea de forma mediata o inmediata. Esto equivale a sostener que no hay ningún abonado que se encuentre aislado de la red generada. De hecho, el diámetro de la red es de 6 pasos mientras que la distancia media entre cualquier par de nodos es de 3,68 pasos.

Sin embargo, la utilidad analítica del gráfico es escasa, por lo que resulta necesario ir desgranando la información a partir de la aplicación de algunos filtros de potencial interés. A raíz de ello es que se confeccionaron las redes de observados, núcleo y frecuente.

Red de observados

El primer filtro utilizado es la de considerar únicamente las comunicaciones que mantuvieron entre sí los abonados observados. En el grafo se aprecian 26 nodos y 19 lazos. A mayor cantidad de comunicaciones mayor es el grosor del lazo que vincula a dos abonados observados.

Esta red permite percibir de forma ágil cómo se vinculan los abonados de interés dentro de la investigación penal. Por otra parte y no menos importante, también permite identificar qué abonados observados no se encuentran asociados de forma directa a la estructura principal de comunicaciones. En este caso particular, se encuentra un componente grande que vincula a 10 abonados observados, un componente pequeño que vincula a 2 y la presencia de 14 abonados de potencial interés pero que, con los datos recolectados, no poseen registros de comunicaciones directas entre sí.

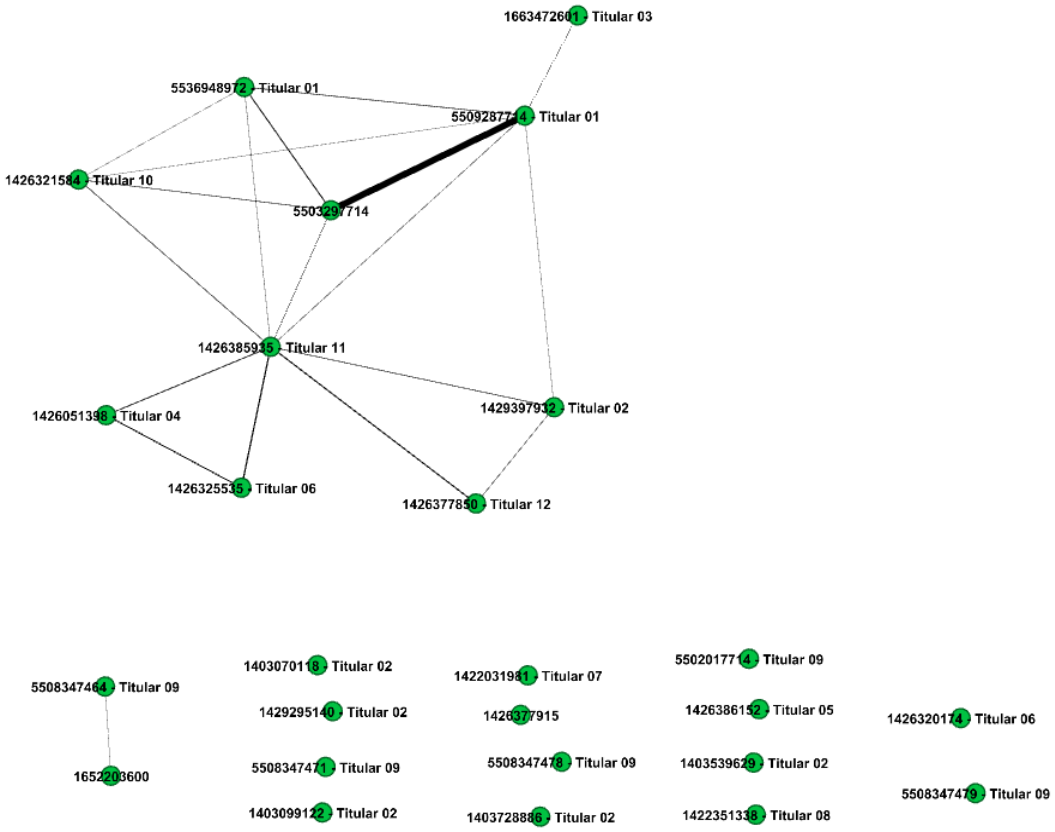


Figura 12 – Grafo de la Red de Observados (esquema de elaboración propia con el software Gephi 0.9.2).

Otra posibilidad es que, si contamos con información sobre la titularidad de los abonados, agrupemos los abonados con idéntica titularidad. Esta operatoria se puede observar en el gráfico a continuación:

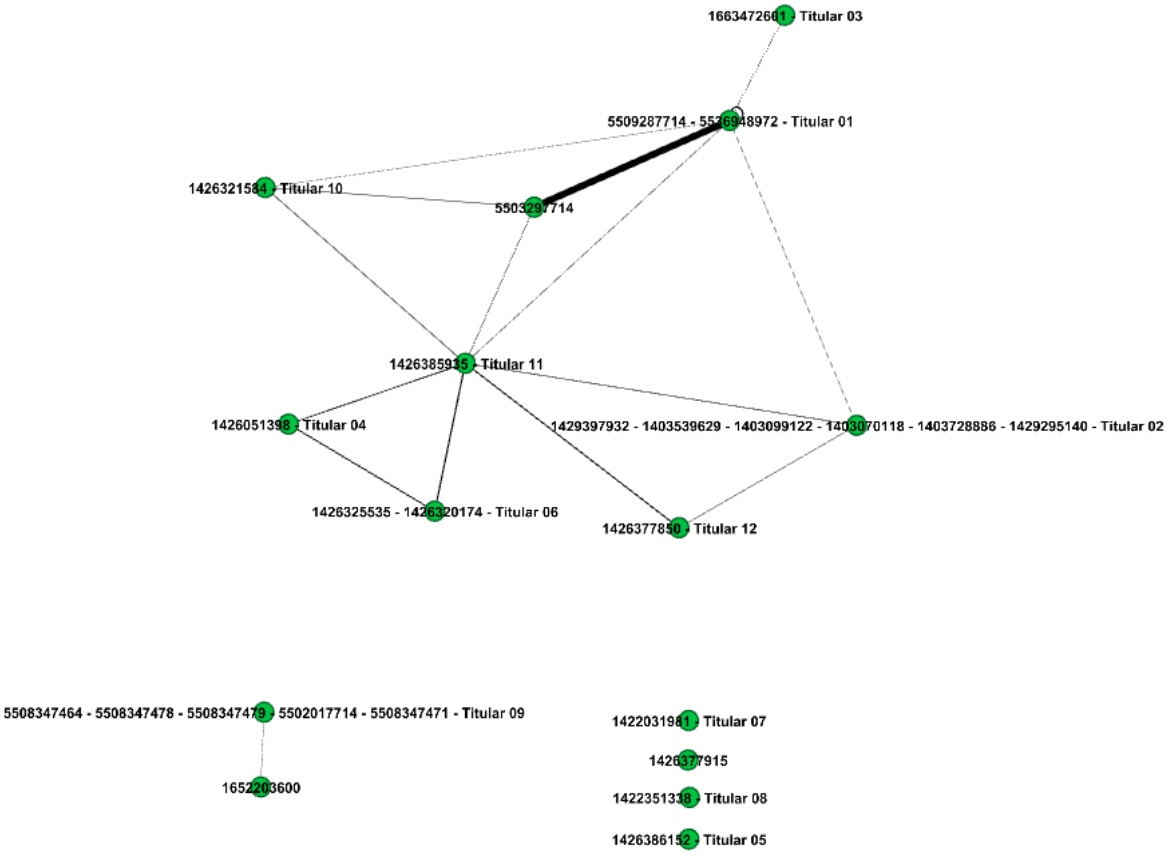


Figura 13 – Grafo de la Red de Observados agrupado por titularidades (esquema de elaboración propia con el software Gephi 0.9.2).

De allí se desprende una red más simple por contar con menos nodos, con una estructura idéntica a la anterior (dos componentes conexos) pero con una menor cantidad de abonados desconectados (pasó de 14 abonados a 4 titulares).

Red Núcleo

La red núcleo es la expresión reticular de la tabla de Abonados Puentes. La misma muestra con nodos de color verde a los abonados observados y en nodos de color rosado a los abonados no observados que cumplen la función de puente, es decir, comunicarse con dos o

más abonados en común. Esta red está compuesta por 83 nodos en total (18 abonados observados y 65 no observados puente) y 177 aristas.

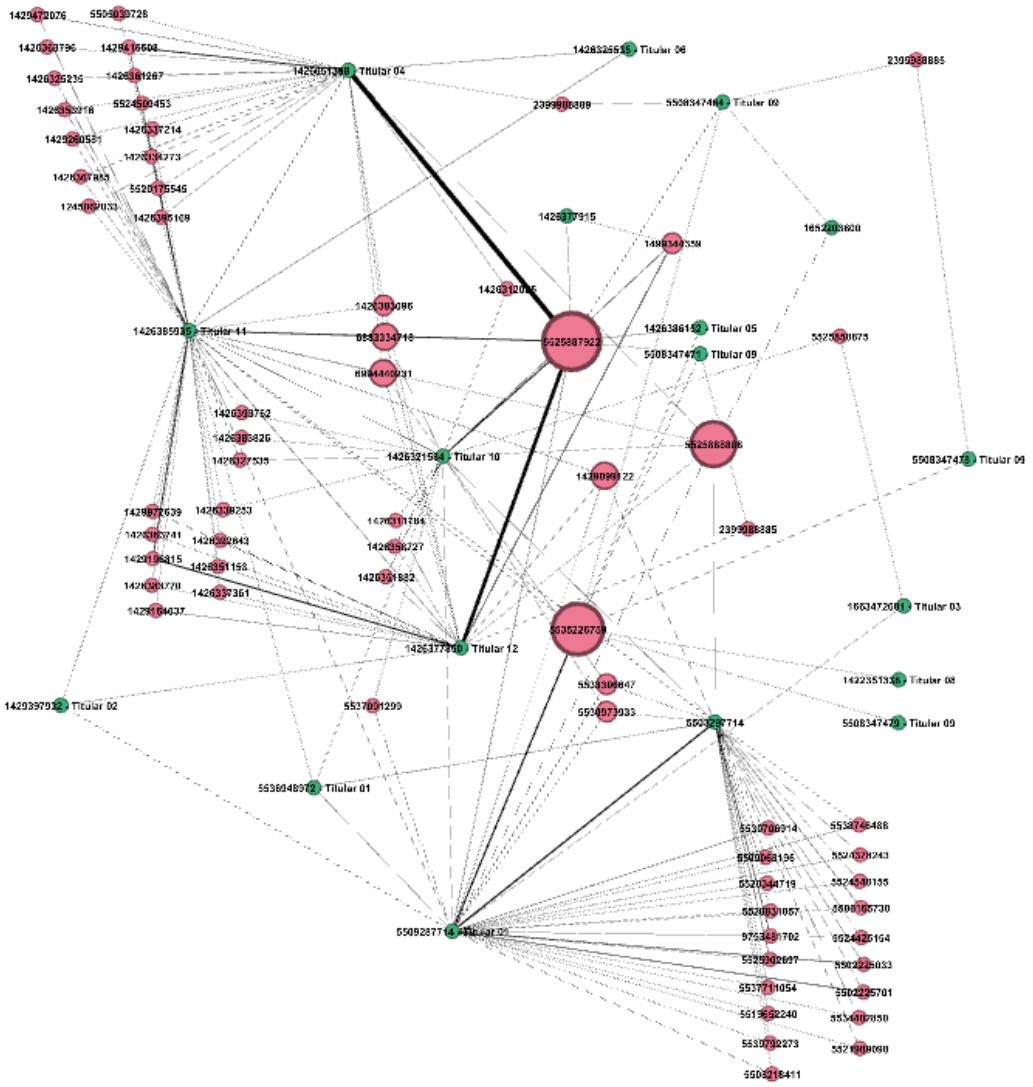


Figura 14 – Grafo de la Red Núcleo (esquema de elaboración propia con el software Gephi 0.9.2).

La primera cuestión a tener en cuenta es que acá sí se pueden vincular abonados observados que mantuvieron comunicaciones indirectas a través de terceros en común con otros

abonados observados y que, por la misma razón, aparecían desconexos en la red de observados.

En segundo lugar, cabe destacar que esta red evidencia la importancia estructural de ciertos abonados no observados que hasta el momento no habían identificados como potencialmente relevantes. En ese sentido, el tamaño mayor de los nodos se corresponde con la cantidad de vinculaciones que mantienen los no observados con los observados. Así se destacan los abonados puente 5525887922, 5535226759 y 5525888888 que registraron comunicaciones con 9, 8 y 7 abonados observados respectivamente.

Red de comunicaciones frecuentes

Otra metodología para identificar abonados no-observados es a través de la frecuencia de sus comunicaciones. Este potencial interés se establece en base a lo que se denomina “vínculos fuertes”, es decir, qué lazos de la red se activan con mayor frecuencia. En el gráfico que se observa a continuación, el punto de corte establecido fue de 100 comunicaciones. Esto significa que solo se ven aquellos nodos y vínculos que representen 100 o más comunicaciones. Bajo estos parámetros, la red está compuesta por 30 nodos en total (8 abonados observados y 22 no observados) y 27 lazos.

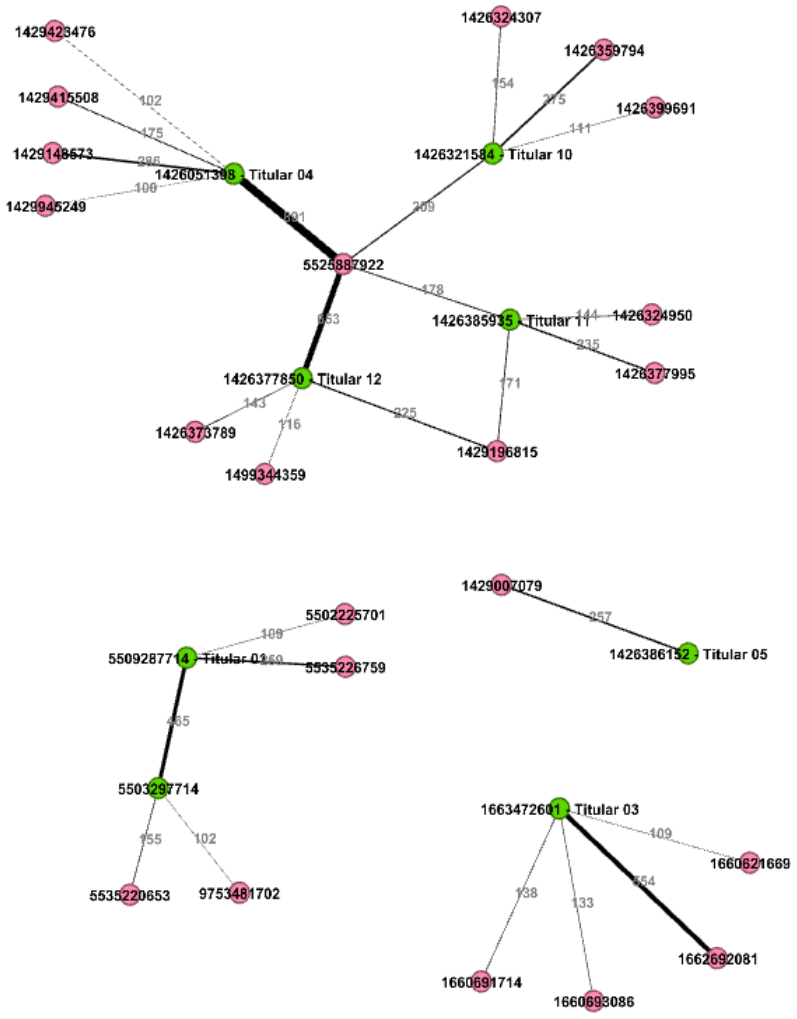


Figura 15 – Grafo de la Red Frecuente (esquema de elaboración propia con el software Gephi 0.9.2).

Cabe destacar que en esta red pueden aparecer los tres tipos de nodos: los observados (como en el caso de las 465 comunicaciones entre los nodos 5509287714 y 5503297714), los no observados puente (como el caso del nodo 5525887922) y, por último, los no observados referidos (como el nodo 1429007079).

Análisis de centralidad: determinando abonados de potencial interés

Otra posibilidad de generar inteligencia aparte de la aplicación de filtros lo constituyen las métricas de análisis a partir de los algoritmos del ARS. De un amplio abanico, los algoritmos más utilizados son los de centralidad. Ellos permiten jerarquizar la importancia de los nodos en base a la estructura de los vínculos registrados. Para ello, se utilizan principalmente dos medidas que permiten evaluar la importancia relativa de un nodo: la centralidad de grado y la centralidad de intermediación.

La centralidad de grado contabiliza cuántos lazos tiene un determinado nodo y sobreentiende que a mayor cantidad de lazos mayor es la importancia del nodo. Es una medición a nivel local del nodo. Por otra parte, la centralidad de intermediación calcula cuántos caminos mínimos de la red pasan por un determinado nodo y, a partir de ello, interpreta que un nodo tiene más centralidad en cuanto pasen por él mayor cantidad de caminos mínimos. Esta segunda definición de centralidad resulta más compleja y contraintuitiva puesto que no se limita a una visión local del nodo sino a una global del conjunto de la red. De esta forma no caracteriza al nodo según cantidad de vínculos sino por la calidad de los mismos, es decir, por la presencia de vínculos estratégicos que lo convierten en un intermediario de la red.

En la Tabla 2 y la Tabla 3 se puede ver un ranking en orden descendente de mayor a menor de los primeros 20 nodos según centralidad de grado y su centralidad de intermediación. Lo importante de observar es la diferencia en el ranking del tipo de nodos según si son observados o no. La centralidad de grado no nos dice mucho sobre nodos potencialmente relevantes que no hayamos tenido en cuenta previamente, puesto que en el ranking hay una preeminencia de los abonados observados. Sin embargo, no ocurre lo mismo con la centralidad de intermediación, donde no solo aparecen más nodos no observados sino que se encuentran mejor rankeados.

Abonado	Tipo	Titular	Grado	Intermediación	Combinada
1652203600	Observado		598	1.069.702,46	1788,800108
1426051398	Observado	Titular 04	439	787606,01	1794,09113

1426377850	Observado	Titular 12	285	517404,0824	1815,452921
1663472601	Observado	Titular 03	212	417.445	1969,082154
1426385935	Observado	Titular 11	175	401934,8053	2296,770316
5509287714	Observado	Titular 01	154	621461,4344	4035,46386
1426321584	Observado	Titular 10	143	253755,1509	1774,511544
5503297714	Observado		115	191.426,66	1664,579617
5508347464	Observado	Titular 09	28	84855,13527	3030,540545
1426386152	Observado	Titular 05	24	37574,7	1565,6125
5508347471	Observado	Titular 09	24	35762,96078	1490,123366
1426377915	Observado		16	25.084	1567,754176
5525887922	No observado		9	117877,0965	13097,45517
*525	No observado		9	39.725	4413,931082
*528	No observado		8	37633,37974	4704,172468
5535226759	No observado		8	34.594	4324,304594
5525888888	No observado		7	928659,5669	132665,6524
*555	No observado		7	98.508	14072,55438
*222	No observado		6	22.282	3713,690999
6994440231	No observado		4	25.465	6366,238064

Tabla 2 – Ranking de abonados ordenado de mayor a menor según centralidad de grado (esquema de elaboración propia).

Abonado	Tipo	Titular	Grado	Intermediacion	Combinada
1652203600	Observado		598	1.069.702,46	1788,800108
5525888888	No observado		7	928659,5669	132665,6524
1426051398	Observado	Titular 04	439	787606,01	1794,09113
5509287714	Observado	Titular 01	154	621461,4344	4035,46386
1426377850	Observado	Titular 12	285	517404,0824	1815,452921
1663472601	Observado	Titular 03	212	417.445	1969,082154
1426385935	Observado	Titular 11	175	401934,8053	2296,770316

1426321584	Observado	Titular 10	143	253755,1509	1774,511544
5503297714	Observado		115	191.426,66	1664,579617
5525887922	No observado		9	117877,0965	13097,45517
*555	No observado		7	98.508	14072,55438
5508347464	Observado	Titular 09	28	84855,13527	3030,540545
*525	No observado		9	39.725	4413,931082
*528	No observado		8	37633,37974	4704,172468
1426386152	Observado	Titular 05	24	37574,7	1565,6125
5508347471	Observado	Titular 09	24	35762,96078	1490,123366
5535226759	No observado		8	34.594	4324,304594
6994440231	No observado		4	25.465	6366,238064
6883334718	No observado		4	25.465	6366,238064
1426377915	Observado		16	25.084	1567,754176

Tabla 3 – Ranking de abonados ordenado de mayor a menor según centralidad de intermediación (esquema de elaboración propia).

Una tercera posibilidad es combinar ambas medidas de centralidad. Para eso generamos un índice de centralidad combinada que se calcula como la razón entre la centralidad de intermediación y la centralidad de grado. Con este cálculo volvemos a generar el ranking de 20 primeros nodos en el cual se observa la mayor presencia de abonados no intervenidos y en los primeros lugares dentro del listado. En este sentido, se puede afirmar que el índice de centralidad combinada constituye el más interesante indicador para identificar abonados potencialmente relevantes que no fueron tenidos en cuenta en la investigación.

Abonado	Tipo	Titular	Grado	Intermediacion	Combinada
5525888888	No observado		7	928659,5669	132665,6524
*555	No observado		7	98.508	14072,55438
5525887922	No observado		9	117877,0965	13097,45517
5525858875	No observado		2	13504	6752
6994440231	No observado		4	25.465	6366,238064
6883334718	No observado		4	25.465	6366,238064
1426383096	No observado		3	15.666	5221,942928
*528	No observado		8	37633,37974	4704,172468

*525	No observado		9	39.725	4413,931082
5535226759	No observado		8	34.594	4324,304594
5509287714	Observado	Titular 01	154	621461,4344	4035,46386
1429099122	No observado		4	14.899	3724,635993
*222	No observado		6	22.282	3713,690999
1426312025	No observado		2	7.340	3670,113795
1429397932	Observado	Titular 02	3	9.968	3322,803045
5508347464	Observado	Titular 09	28	84855,13527	3030,540545
2399988889	No observado		2	4.680	2340,221514
1426385935	Observado	Titular 11	175	401934,8053	2296,770316
1663472601	Observado	Titular 03	212	417.445	1969,082154
1426377850	Observado	Titular 12	285	517404,0824	1815,452921

Tabla 4 – Ranking de abonados ordenado de mayor a menor según centralidad combinada (esquema de elaboración propia).

4 - Conclusiones

Resulta ineludible que, en el ámbito de la investigación penal, nos encontramos ante un cambio de época. Ya se trate de una pose coyuntural o de un profundo convencimiento, lo cierto es que todas las personas involucradas en los organismos policiales y de administración de justicia expresan la necesidad de incorporar nuevos conocimientos, procedimientos, metodologías y perspectivas que permitan abordar las investigaciones penales. No se trata de acumular más o mejor información, sino de poder procesarla y analizarla para obtener conocimiento.

Justamente este fue el marco general que define mi trabajo, el del análisis de la inteligencia criminal, entendido como el espacio donde se intersectan las problemáticas en materia de investigación penal, las metodologías de las ciencias sociales y los procedimientos y técnicas computacionales de análisis. En ese sentido, si el objetivo de la explotación de datos es descubrir patrones relevantes a partir de grandes volúmenes de información almacenada, sin lugar a dudas el ARS tiene reservado por derecho propio un lugar dentro de las técnicas más productivas de inteligencia criminal.

De todas formas, el verdadero desafío no es demostrar que determinada herramienta es útil para la producción de inteligencia criminal, sino que esa producción sea institucional, comunicable y, por ende, formalizada. Por esta razón se buscó generar un proceso experto pero explícito, trazable y reproducible, lejos de las jergas crípticas, las cajas negras o los conocimientos tácitos.

Para llevar a cabo este enfoque utilicé como ordenador del trabajo los pasos del ciclo de inteligencia criminal. El desarrollo realizado en este trabajo se inspiró fuertemente en dicha perspectiva, pasando primero por la toma de datos donde se analizaron las diferentes fuentes de comunicaciones como así también sus pros y sus contras. Luego continué con el procesamiento de los datos mediante transformaciones necesarias para consolidar la información. Y, por último, la etapa de análisis donde aplicamos tanto filtros como métricas propias de los algoritmos del ARS.

Espero que con este trabajo se aprecie un esfuerzo, entiendo yo, necesario de desarrollo y estandarización de una metodología de trabajo para realizar cruces de información telefónica con el fin de aprovechar la multiplicidad de datos disponibles. Este esfuerzo no solo tiene que ver con recuentos de frecuencias aplicados con diferentes criterios, sino que apunta además a un valor agregado específico. En ese sentido, se describió como el ARS se entronca en una importante relación con la investigación penal, lo que produjo por lo menos tres mojones criminológicos importantes: la relevancia de las interacciones débiles, la detección sofisticada de entidades centrales y el análisis de la topología de la red con sus efectos en el diseño de intervenciones.

A pesar del desarrollo teórico-metodológico resulta un hecho palpable que la perspectiva no se encuentra ampliamente incorporada como uno esperaría. Por el contrario, se identificaron tres dificultades en la adopción del ARS. La primera refiere a la intención de utilizar software específico como reemplazo del analista de redes. La segunda está relacionada con la posibilidad de manejar volúmenes de información cada vez más extensos. Y la tercera está en relación con la falta de formación específica en la epistemología y la metodología del ARS.

Entiendo que la utilización del ARS como herramienta de inteligencia criminal para el estudio de las comunicaciones telefónicas en investigaciones penales se encuentra más que fundamentado. Solo falta, como cualquier novedad que se precie de traer consigo beneficios, persuadir a los no convencidos. Para ello resulta importantísima la retroalimentación continua entre el ARS y diversos casos de aplicación concreta que permitan evaluar la herramienta o, en otras palabras, para que se genere "una dinámica capaz de modificar, de modo iterativo, las hipótesis de base antes que tratar de que la evidencia disponible concuerde invariablemente con el modelo" (Miceli et al, 2016:144). Solo así, con demostraciones a base de trabajo, se podrá consolidar el ARS como estándar y, posteriormente, buscar expandir su frontera de potencialidades y conocimientos.

5 - Bibliografía

- **Aggarwal**, **Charu C**. (2018) "Social network analysis in counterterrorism", Encyclopedia of SNA and Mining, Springer.

- **Britos**, **P.**, **Fernández**, **E.**, **Merlino**, **H.**, **Pollo-Cataneo**, **F.**, **Rodríguez**, **D.**, **Procopio**, **C.**, **Rancan**, **C.**, **García-Martínez**, **R**. (2008) "Explotación de información aplicada a inteligencia criminal en Argentina".

- **Burcher**, **M.**, **Whelan**, **C**. (2017) "Social network analysis as a tool for criminal intelligence: understanding its potential from the perspectives of intelligence analysts", Trends Organ Crim, DOI 10,1007/s12117-017-9313-8.

-**Calderoni**, **F.** (2012) "The structure of drug trafficking mafias", Crime Law and Social Change, 58 (3).

- **Campana**, **P.**, **Varese**, **F.** (2011) **"**Listening to the wire - criteria and techniques for the quantitative analysis of phone intercepts", Trends in Organized Crime, 15(1), 13-30.

- **Catanese**, **S.**; **Ferrara**, **E.**; **Fiumara**, **G.** (2013) "Forensic analysis of phone call networks", Social Network Analysis and Mining, Vol. 3 N° 1, Springer, ISSN 1869-5450. **http://www.emilio.ferrara.name/wp-content/uploads/2011/06/SNAM-2011.pdf** (última vez revisado 09-11-19).

- **Chen**, **H.**, **Chung**, **W.**, **Xu**, **JJ.**, **Wang**, **G.**, **Qin**, **Y.**, **Chau**, **M**. (2004) "Crime data mining: a general framwork and some examples", Computer, v.37 n. 4, p. 50-56.

- **Duijin**, **PAC.**, **Klerks**, **PPHM**. (2014) "Social network analysis applied to criminal networks: recent developments in Dutch law enforcement", Masys AJ (ed) Networks and network analysis for defense and security, Springer, Heidelberg, pp 121-159.

- **Galessio**, **E.** (sin fecha) "El aporte de la inteligencia criminal a la seguridad pública" en https://es.scribd.com/document/37779336/El-aporte-de-la-inteligencia-criminal-a-la-seguridad-publica (última vez revisado 10-11-19).

- **Guariglia**, **F.** (2016) "Que hacer con la investigación penal y con el ministerio público", Revista Argentina de Teoría Jurídica, Vol. 17, Buenos Aires, Argentina. utdt.edu/download.php?fname=_147670263504682100.pdf (ultima vez revisado 09-11-19).

- **Hanneman**, **R**. (2000) "Capítulo Primero: Los datos de las redes sociales", Introducción a los métodos del análisis de redes sociales. http://revistaredes.rediris.es/webredes/textos (ultima vez revisado 09-11-19).

- **Harper**, **WR**.; **Harris**, **DH**. (1975) "The application of Link Analysis to Police Intelligence", Human Factors, 17 (2), 157-164.

- **Hopkins**, **A.** (2010) "Graph theorym, social networks and counter terrorism", University of Massachusetts, Darmouth.

- **Karthika**, **S**., **Bose**, **S**. (2011) "A comparative study of social networking approaches in identifying the covert nodes", International Journal on Web Service Computing (IJWSC), Vol. 2, No. 3.

- **Klerks**, **P.** (2001) "The network paradigm applied to criminal organizations: theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands", Conenections 24(3): 53-65.

- **Krebs**,**VE**. (2002a) "Mapping networks of terrorist cells", Connections 24(3): 43-52, INSNA.

- **Krebs**,**VE**. (2002b) "Uncloaking terrorist networks", First Monday, Volume 7 Number 4.

- **Lu**, **Y.**; **Luo**, **X.**; **Polgar**, **M.**; **Cao**, **Y.** (2010) "Social network analysis of a criminal hacker community", Journal of Computer Information Systems.

- **Martínez**, **AM**. (2017) "Enfoques metodológicos en el análisis criminal: de la estadística clásica al análisis de redes sociales", ponencia presentada en la mesa "Seguridad en agenda" en las III Jornadas Interdisciplinarias de Jóvenes Investigadores en Ciencias Sociales IDAES-UNSAM, San Martín, Buenos Aires.

-**McGloin**, **JM.** (2005) "Policy and intervention considerations of a network analysis of street gangs", Criminology and Public Policy, 4, 3; Proquest.

- **Miceli**, **J**.; **Orsi**, **O**.; **Rodríguez García**, **N**., (2016) "Análisis de redes sociales y sistema penal", Valencia, Tirant Lo Blanche.

- **Morris**, **JF**.; **Deckro**, **RF**. (2013) "SNA data difficulties with dark networks", Behavioral Sciences of Terrorism and Political Aggression, Vol. 5, No. 2, 70-93.

- **Morselli**, **C**. (2009) "Inside criminal networks", New York, Springer.

- **Morselli**, **C**. (2010) "Assessing Vulnerable and Strategic Positions in a Criminal Network", Journal of Contemporary Criminal Justice, v. 26, pp. 382-392.

- **Navarro**, **MAE., Navarro Bonilla**, **D.** (2003) "Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información" en El Profesional de la Información, v.12, n.4.

- **Papachristos**, **AV**. (2009) "Murder by structure: dominance relations and the social structure of gang homicide", University of Chicago.

- **Pezzuchi**, **G.** (2017) "Clase 1", Análisis del Delito II, Carrera de Especialización en Criminología, Universidad Nacional de Quilmes.

- **Reynoso**, **C.** (2011) "Redes sociales y complejidad, Modelos interdisciplinarios en la gestión sostenible de la sociedad y la cultura", Editorial SB, Buenos Aires, Argentina.

- **Sarvari**, **H.**; **Abozinadah**, **E.**; **Mbaziira**, **A.**; **McCoy**, **D.** (2014) "Constructing and analyzing criminal networks". IEEE Security and Privacy Workshop.

- **Sparrow**, **M**. **K**. (1991) "The application of network analysis to criminal intelligence: An assessment of the prospects", Social Networks, v. 13, pp. 251-274.

- **van der Hulst**, **RC**. (2009) "Introduction to social network analysis (SNA) as an investigative tool", Springer, Trends Organ Crim 12:101-121.

- **Villedieu**, **J**. (2015) How to use phone calls and network analysis to identify criminals? en https://linkurio.us/blog/how-to-use-phone-calls-and-network-analysis-to-identify-criminals/ (ultima vez revisado 06-09-2017)

- **Wasserman**, **S.;** y **Faust**, **K.** (1994) "Social Network Analysis: Methods and Applications", Cambridge University Press, Cambridge.

- **Will**, **UK.** (2013) “Issues fot the next generation of criminal network investigation tool”, European intelligence and security informatics conference.

- **Xu**, J., y **Chen**, H. (2008) “The topology of dark networks”, Communications of the ACM.