



12º CONGRESO ARGENTINO DE ANTROPOLOGÍA SOCIAL

La Plata, junio y septiembre de 2021

GT69. Antropología aplicada y modelos complejos: expandiendo la frontera metodológica

Indicadores reticulares para la detección de abonados telefónicos potencialmente relevantes en el marco de investigaciones judiciales

Alejandro Manuel Martínez. Facultad de Filosofía y Letras, Universidad de Buenos Aires. Dirección General de Investigaciones y Apoyo Tecnológico (DATIP), Procuración General de la Nación. martinezale1987@gmail.com

Resumen

En el marco de las investigaciones judiciales, resulta habitual la utilización de datos de telecomunicaciones como fuente de información preliminar y/o probatoria sobre grupos de criminalidad compleja. Los agentes judiciales, en gran medida, están acostumbrados a la recolección de datos telefónicos, pero no así a su procesamiento y análisis. Esta situación se agrava más día a día con la explosión de grandes volúmenes de información.

Para dar respuesta a esta dificultad, y dentro de una dependencia judicial abocada al desarrollo de pericias interdisciplinarias para el apoyo a la investigación penal, se conformó un equipo al cual pertenezco que realiza procedimientos de preparación y consolidación de la información a través de bases de datos relacionales y los analiza posteriormente mediante el análisis de redes sociales (ARS).

Dado que una de las características específicas de las redes criminales está dada por el hecho que los actores dentro de un grupo criminal procuran no dejar rastros de sus interacciones, la utilización de indicadores reticulares provee de trazabilidad,



eficiencia y rigurosidad, todos ellos valores que no se pueden obviar por ser relevantes en el proceso penal.

En ese sentido, los algoritmos de centralidad parecen vincularse de forma específica con determinados roles dentro de una organización criminal. La centralidad de grado es el indicador más intuitivo y se correlaciona con aquellos actores más visibles para el accionar judicial. La centralidad de intermediación, al ser una medida dependiente de la estructura global de la red, resulta ya más difícil de elucidar para el operador judicial, brindando información de potencial interés. Por último, la conjunción de ambos brinda el índice de centralidad combinada cuyo objetivo es detectar “jugadores claves”, es decir, aquellos nodos con pocos vínculos, pero de mayor calidad, arrojando los resultados más interesantes por contraintuitivos y, por ende, la más provechosa fuente de información para la investigación penal.

Palabras clave: *análisis de redes sociales, comunicaciones telefónicas, criminología, investigación judicial.*

Introducción: criminología y análisis de redes sociales

El desafío de llevar adelante causas de criminalidad compleja no se caracteriza por la dificultad de incorporar datos, sino por la incapacidad de aprehenderlos y extraer conocimiento útil de ellos. Es así como las prácticas de investigación penal abocadas a la criminalidad compleja no se pueden limitar al conocimiento jurídico. La necesidad de procesar y analizar datos, tanto masivos como heterogéneos, constituye un forzante para incorporar otras disciplinas en los equipos penales. Actualmente, no resulta extraño encontrar perfiles provenientes de las ciencias sociales o de las ciencias computacionales tanto en las dependencias judiciales como en las fuerzas de seguridad.

En el marco de lo que se conoce como inteligencia criminal, el objetivo de los equipos multidisciplinarios es responder ¿quién?, ¿qué? y ¿con quién? al analizar eventos delictivos. El eje central lo constituyen las relaciones entre personas y grupos involucradas en actividades de naturaleza organizada. Con estas preguntas, el analista 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.

El análisis 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).

Si bien existen antecedentes más antiguos (ver Martínez 2020), la conjunción moderna entre el ARS e inteligencia criminal se inició 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 afirmó 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)

A su vez, Sparrow encontró dos límites en la utilización del ARS en ámbitos de investigación penal: el primero relacionado a la noción de que el objetivo último de estas técnicas era la “ayuda pictórica” en el descubrimiento de patrones; el segundo, la verificación de que, en última instancia, el análisis de inteligencia continuaba dependiendo de procedimientos artesanales y heurísticos de los analistas. Estos límites, hoy en día, continúan reproduciéndose en el seno de las investigaciones penales.

Sin lugar a dudas, el trabajo de Sparrow significó una apertura programática desafiante pero, a pesar de ello, durante la década del 90 no se registraron trabajos académicos que traten la vinculación entre el ARS y la criminología. Hubo que esperar el desarrollo tecnológico y el nuevo contexto mundial después de los

atentados a las Torres Gemelas para que se consolidara el ARS como herramienta de inteligencia criminal (Martínez, 2020). Después del nuevo milenio, el ARS incluyó 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.

En lo que respecta a las telecomunicaciones, si bien en el texto fundacional de Sparrow se las menciona, recién en los últimos tiempos se realizaron 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 insumo de telecomunicaciones haya sido apartado de su tratamiento en red en investigaciones penales, aunque sí se puede aseverar que dicho conocimiento no fue explicitado debidamente. Los trabajos académicos específicos que dan cuenta sobre los procedimientos metodológicos y las problemáticas a resolver al momento de analizar telecomunicaciones han aparecido recién durante la última década.

El primero de dichos desarrollos fue el trabajo de Catanese, Ferrara y Fiumana (2011). Allí, los investigadores sostuvieron 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).

Otro artículo en donde se conjuga ARS y comunicaciones telefónicas lo escribieron Campana y Varese. En referencia a las técnicas de análisis de este tipo de información, los autores sostuvieron 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 enfatizaron 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:

“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).

Un último aporte interesante es el de Villedieu, quién utilizó el concepto de red no sólo en términos de ARS sino también como modelo mismo de la base de datos (Villedieu, 2015). 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.

Indicadores reticulares para la detección de abonados relevantes

En la intersección entre ARS e inteligencia criminal, una de las principales contribuciones criminológicas es la detección de entidades centrales o “*key players*”, donde se pone énfasis en el análisis de los nodos de una red. 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.

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 (Sparrow, 1991), 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 criminal, identifica a las personas más vulnerables de las mismas por estar más expuestas a la mirada del sistema penal de justicia.

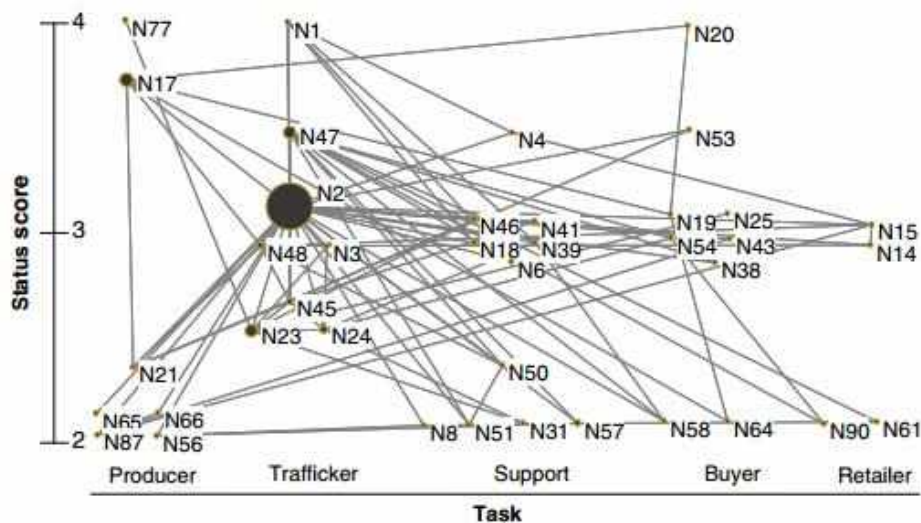


Figura 1 - Red de la organización narcotraficante Chaloneri en Italia. En el eje horizontal se indican los roles de las personas investigadas mientras que en eje vertical se mide su status. El tamaño menor o mayor de los nodos está en función de la centralidad de grado. Se puede observar como ninguno 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. En ese sentido, 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. Según Calderoni,

“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 el resultado de sus interacciones. 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.

Caso de aplicación: detección de abonados telefónicos potencialmente relevantes

A modo de ejemplo, voy a presentar un caso real de aplicación de estos conceptos en el marco de una solicitud de colaboración judicial. Allí se solicitó analizar el flujo de comunicaciones de una asociación criminal acusada de suprimir el estado civil de un menor. Específicamente, se requirió detectar nuevos abonados no observados que sean de potencial interés para la investigación en curso. Para ello, se aportó la información asociada de las telecomunicaciones correspondientes a 26 abonados investigados en un rango temporal de dos meses. Dicha información constituyó un total de 20 archivos de información de prestatarias de servicios telefónicos en las que se registraron 22.745 comunicaciones.

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:

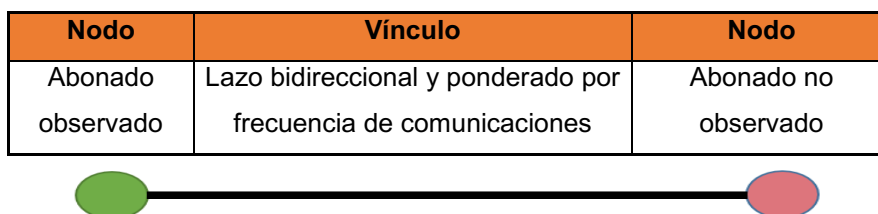


Figura 2 – Modelo de díada que constituye la unidad mínima de la red.

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 rosado 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 de los algoritmos de ARS utilizados. Por otra parte, ponderamos los lazos de comunicaciones por la frecuencia de las mismas. Según nuestra definición de díadas, entendemos que en el modelo de red se pueden tipificar los nodos de la siguiente forma:

- nodos o abonados observados: generalmente son los originantes de la información y suelen ser de interés para la hipótesis de acusación.
- nodos o abonados no observados: son todos aquellos abonados interlocutores de los abonados observados. Pueden presentar dos características:
- nodos o abonados no observados puente: son todos aquellos que se comunican con dos o más nodos abonados observados.
- nodos o abonados no observados referidos: son todos aquellos que solo se comunican con un abonado observado.

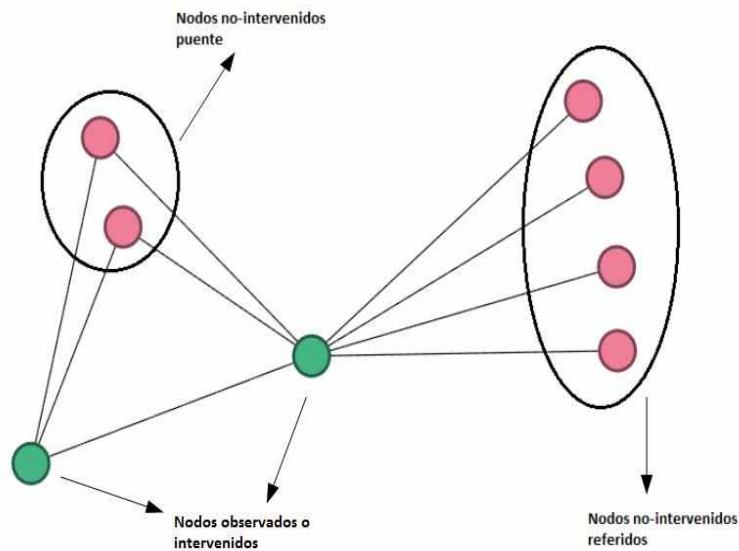


Figura 3 – Modelo de red de comunicaciones para nodos observados, no observados puente y no observados referidos.

Respecto a la información de este caso, el grafo contiene 2094 nodos y 2216 vínculos. La red 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.

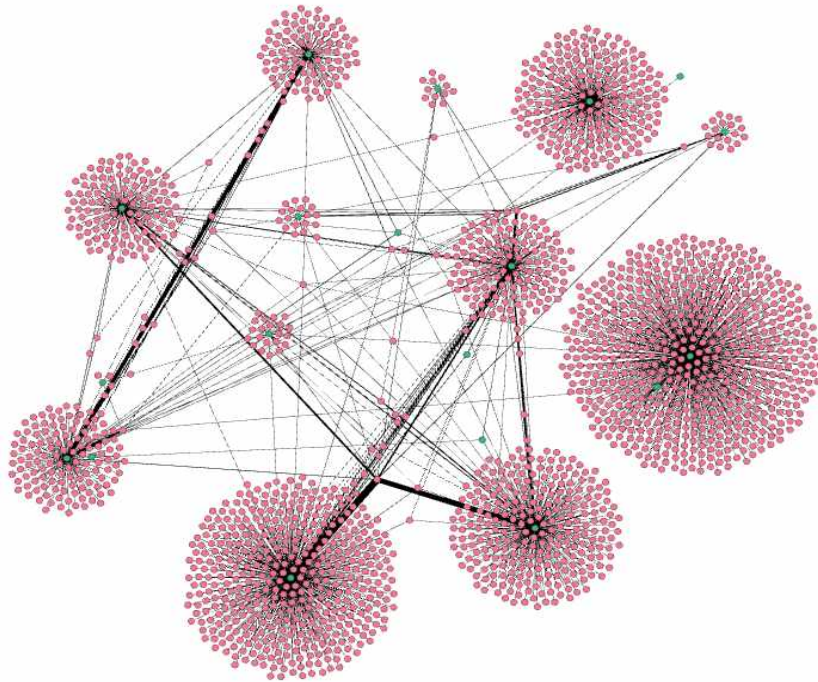


Figura 4 – Grafo de la red Total elaborado con Gephi 0.9.2.

En referencia a los nodos del grafo, se corrieron los algoritmos de centralidad de grado y de intermediación y se volcó toda la información a una tabla¹. De hecho, en la Tabla 1 y la Tabla 2 se puede apreciar 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.

Cabe destacar que la centralidad de grado no aporta mucha información 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.

¹ Los datos de identificación de los abonados telefónicos han sido modificados debido a la sensibilidad de la información. Solo se conservó la cantidad de nodos y sus relaciones.

Abonado	Tipo	Grado	Intermediación	Combinada
1652203600	Observado	598	1.069.702,46	1788,800108
1426051398	Observado	439	787606,01	1794,09113
1426377850	Observado	285	517404,0824	1815,452921
1663472601	Observado	212	417.445	1969,082154
1426385935	Observado	175	401934,8053	2296,770316
5509287714	Observado	154	621461,4344	4035,46386
1426321584	Observado	143	253755,1509	1774,511544
5503297714	Observado	115	191.426,66	1664,579617
5508347464	Observado	28	84855,13527	3030,540545
1426386152	Observado	24	37574,7	1565,6125
5508347471	Observado	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 1 – Ranking de abonados ordenado de mayor a menor según centralidad de grado.

Abonado	Tipo	Grado	Intermediación	Combinada
1652203600	Observado	598	1.069.702,46	1788,800108
5525888888	No observado	7	928659,5669	132665,6524
1426051398	Observado	439	787606,01	1794,09113
5509287714	Observado	154	621461,4344	4035,46386
1426377850	Observado	285	517404,0824	1815,452921
1663472601	Observado	212	417.445	1969,082154
1426385935	Observado	175	401934,8053	2296,770316
1426321584	Observado	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	28	84855,13527	3030,540545

*525	No observado	9	39.725	4413,931082
*528	No observado	8	37633,37974	4704,172468
1426386152	Observado	24	37574,7	1565,6125
5508347471	Observado	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 2 – Ranking de abonados ordenado de mayor a menor según centralidad de intermediación.

Posteriormente, generamos una tercera variable combinando ambas medidas de centralidad. El índice de centralidad combinada se calcula como la razón entre la centralidad de intermediación y la centralidad de grado. Con este se volvió a generar el ranking de 20 primeros nodos.

Abonado	Tipo	Grado	Intermediación	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	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	3	9.968	3322,803045
5508347464	Observado	28	84855,13527	3030,540545
2399988889	No observado	2	4.680	2340,221514
1426385935	Observado	175	401934,8053	2296,770316
1663472601	Observado	212	417.445	1969,082154
1426377850	Observado	285	517404,0824	1815,452921

Tabla 3 – Ranking de abonados ordenado de mayor a menor según centralidad combinada.

Se puede observar la mayor presencia de abonados no intervenidos y en los primeros lugares dentro del listado. En este sentido, el índice de centralidad combinada constituye el más interesante indicador para identificar abonados potencialmente relevantes que no fueron tenidos en cuenta en la investigación.

Conclusiones

En el ámbito de la inteligencia criminal, el análisis de redes sociales presenta un recorrido y una casuística que se viene profundizando desde hace por lo menos 30 años. Sin lugar a dudas, constituye una herramienta fructífera en la investigación penal para tratamiento de información relacional.

Uno de sus aportes centrales es la identificación de nodos de potencial interés investigativo. Para ello se presentaron dos algoritmos de centralidad junto con un índice que los combinada, como así también una interpretación sobre su significado empírico en el dominio criminológico. Es así como el grado nodal se considera como una medida que no refleja la importancia de un nodo dentro de una organización criminal, sino más bien lo contrario, la mayor exposición a la mirada del sistema penal. De forma distinta, el grado de intermediación constituye una medida más contraintuitiva puesto que no se limita a una visión local del nodo sino a una global de la red. Esto posibilita caracterizar a los nodos no por cantidad de vínculos, sino por la calidad de los mismos a la hora de conocer y manipular los flujos de información.

A pesar de ellos, numerosas veces las personas de estatus alto dentro de una organización criminal no se pueden identificar por ninguna de las anteriores medidas. Para ello se utiliza el índice de centralidad combinada, procurando resaltar aquellos nodos que tienen pocos vínculos, pero de muy buena calidad, lo que les permite obtener un posicionamiento estratégico dentro de la red.

En el caso de estudio presentado, que tiene la especificidad de utilizar como insumo los registros telefónicos provistos por las prestatarias de servicios de telecomunicaciones, las articulaciones criminológicas planteadas entre los diferentes indicadores de centralidad se cumplían. En definitiva, el índice de centralidad

combinada fue el más útil para identificar abonados telefónicos potencialmente relevantes para la investigación penal.

Referencias Bibliográficas

- 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 framework and some examples", Computer, v.37 n. 4, p. 50-56.
- Duijijn, 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.
- Hopkins, A. (2010) "Graph theory, social networks and counter terrorism", University of Massachusetts, Dartmouth.
- 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", *Conenectons* 24(3): 53-65.
- Krebs, V.E. (2002a) "Mapping networks of terrorist cells", *Connections* 24(3): 43-52, INSNA.
- Krebs, V.E. (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, A.M. (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.
- Martínez, A.M. (2020) "Análisis de redes, comunicaciones telefónicas e investigación penal. Un aporte metodológico en análisis de inteligencia criminal", Trabajo Final Integrador de Especialización en Criminología, Universidad Nacional de Quilmes, Bernal, Argentina. <http://ridaa.unq.edu.ar/handle/20.500.11807/2637>
- McGloin, J.M. (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, J.F.; Deckro, R.F. (2013) "SNA data difficulties with dark networks", *Behavioral Sciences of Terrorism and Political Aggression*, Vol. 5, No. 2, 70-93.
- Morselli, C. (2010) "Assessing Vulnerable and Strategic Positions in a Criminal Network", *Journal of Contemporary Criminal Justice*, v. 26, pp. 382-392.
- Papachristos, A.V. (2009) "Murder by structure: dominance relations and the social structure of gang homicide", University of Chicago.
- 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, R.C. (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)
- Will, UK. (2013) "Issues for the next generation of criminal network investigation tool", European intelligence and security informatics conference.