—ENSAYO—

OSINT y análisis de datos en inteligencia e investigación criminal: herramientas, técnicas y desafíos

OSINT and data analysis in criminal intelligence and investigations: tools, techniques and challenges

Martín Ignacio Estrabou

Especialista en Inteligencia Estratégica y Crimen Organizado (UBA). Lic. en Relaciones Internacionales (UADE). Exdirector de Análisis Narcocriminal, Ministerio de Seguridad y Justicia de Río Negro.

Recepción: 23/3/2025 | Aprobación: 2/5/2025

Resumen

El presente ensayo propone describir de forma general las herramientas y técnicas necesarias para la producción de inteligencia e investigaciones criminales ante el flujo de información generado por las organizaciones delictivas en la sociedad de la información.

El mismo se encuentra estructurado en cuatro partes. Primero, una introducción que contextualiza las actuales amenazas transnacionales. Luego, en la segunda parte, se conceptualiza y establecen las diferencias entre inteligencia e investigación criminal. Posteriormente, se presentan las herramientas tecnológicas y metodologías, clasificadas por su disciplina y operatoria. Finalmente, se exponen conclusiones sobre desafíos humanos y logísticos en la lucha contra el crimen organizado.

Palabras clave: análisis; técnicas; inteligencia; investigación.

Abstract

This essay aims to provide a general overview of the tools and techniques required for the production of criminal intelligence and investigative processes in order to give answer to the volumen of information generated by criminal organizations in the information society.

The paper is structured into four parts. The first part is an introduction that contextualizes current transnational threats. The second section defines and differentiates the concepts of intelligence and criminal investigation. The third part presents technological tools and methodologies, classified by discipline and application. Finally, conclusions and challenges are presented.
Keywords: *analysis; techniques; intelligence; investigation.*

Introducción

La compleja dinámica del contexto global actual en materia de seguridad y defensa exige que los Estados enfrenten distintos riesgos y amenazas. Por un lado, se está en presencia de un sistema internacional multipolar con focos activos de enfrentamientos directos entre Estados, como el conflicto entre Rusia y Ucrania, o Israel y Palestina. Por otro lado, y en línea con el objeto de estudio de este trabajo, la multiplicidad de actividades ilícitas donde las amenazas provienen de actores no estatales, siendo conflictos de esencia híbrida donde se combinan grupos civiles organizados de distintas regiones interdependientes entre sí.

El monopolio de la violencia estatal se encuentra entonces desafiado por grupos delictivos organizados que cometen delitos graves en el tiempo con el fin de obtener directa o indirectamente un beneficio económico o material (Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos, 2000[1]). En la actualidad, según datos del Global Organized Crime Index elaborado por la Global Initiative Against Transnational Organized Crime (GI-TOC, 2023), a nivel global los mercados ilegales con mayor prevalencia en donde actúan estos tipos de grupos son los delitos financieros, tráfico de personas, tráfico de cannabis, tráfico de armas y contrabando. Luego se ubica el tráfico de otros estupefacientes y los delitos cibernéticos.

La naturaleza de cada delito es distinta por su temática, relevancia, *modus operandi* e impacto. Además, algunos de ellos en tendencia al alza se van tecnificando, por ejemplo, los delitos financieros, que empiezan a bucear en otros entornos distintos al tradicional para ofuscar dinero, o los ciberdelitos, que van modificando nuevas formas de *malware* para el robo o secuestro de datos.

En este marco, el esfuerzo y dedicación que demanda la persecución de la criminalidad organizada plantea desafíos para las Gobiernos y decisores de la política criminal y de seguridad, tanto para la detección como la anticipación de estos. Por ello, la profesionalización de los investigadores y auxiliares de la justicia en el uso de herramientas tecnológicas avanzadas resulta fundamental para la recolección,

[1] También conocida como Convención de Palermo, es un acuerdo internacional que establece un marco legal para el combate del crimen organizado.

procesamiento e interpretación de información, permitiendo así la generación de inteligencia criminal proactiva y evidencia sólida en procesos penales.

1. Inteligencia e investigación criminal

El concepto de inteligencia, del cual derivó posteriormente en las distintas ramas como la criminal, tiene su origen esencialmente en la inteligencia militar. El considerado padre de la inteligencia moderna y quien le dio un marco científico, Sherman Kent (1966), la definió como «conocimiento que nuestros hombres, civiles y militares, que ocupan cargos elevados, deben poseer para salvaguardar el bienestar nacional» (p. 3). Más allá de la generalidad del concepto, es pertinente destacar que cimentó las bases metodológicas que posteriormente se desarrolló en el denominado ciclo de inteligencia, donde se plantean cuatro etapas: dirección, obtención, proceso y difusión.

En relación con el objeto del ensayo, previamente a definir el concepto de inteligencia criminal, es menester distinguirlo de la investigación criminal y comprenderlos como conceptos cuya misión y objetivos son distintos, pero correlacionados entre sí. La inteligencia criminal es parte de la actividad policial y de seguridad pública que utiliza metodologías de la disciplina para el análisis en sus tres niveles: estratégico, operacional y táctico (Ugarte, 2024).

El nivel estratégico enfocado al conocimiento del estado de situación, antecedentes, tendencias, riesgos y amenazas, con la finalidad de implementar acciones y estrategias proactivas que puedan anticipar cualquier acontecimiento o conductas antijurídicas. El mismo es formulado a nivel ministerial y es el que elabora la política de seguridad a seguir estableciendo medidas a corto, mediano y largo plazo.

En cuanto al nivel operacional, está vinculado con aquellas acciones llevadas a cabo por rangos medios en sus correspondientes jurisdicciones en pos de reducir el delito. Incluye una aproximación más cercana al terreno, la planificación eficiente en la asignación de recursos y el despliegue de estos.

Por su parte, el nivel táctico puntualiza un objetivo determinado sobre un tipo de delito específico o bandas criminales en acción. En este nivel es donde se encuentran los actores que actúan como investigadores en el campo: jueces, fiscales, fuerzas de seguridad, agencias específicas, entre otros; y donde se relaciona con el concepto previamente presentado de investigación criminal.

Ahora bien, investigación criminal *per se* hace referencia a la recolección de pruebas durante un proceso penal, inquisitorio o acusatorio según el marco jurídico, para esclarecer un hecho delictual específico e identificar sus responsables. Entonces, mientras que en inteligencia criminal se busca comprender el fenómeno delictual desde

una visión más operativa como la composición de una banda, *modus operandi*, ubicación geográfica, antecedentes, etc., la investigación se centra sobre un hecho determinado por ser considerado *ab initio* como delito.

2. Técnicas y herramientas analíticas para la producción de inteligencia e investigación criminal

2.1. OSINT

Según Block (2024), Open-Source Intelligence es «la recopilación metódica y explotación de información proveniente de fuentes públicas para satisfacer un requerimiento de inteligencia» (p. 97). Fuentes públicas refiere a todo lo que está disponible en Internet sin restricciones legales ni barrera de autorización. Algunos ejemplos son los motores de búsqueda, información pública gubernamental, foros y plataformas, redes sociales donde el usuario o suscriptor posea una cuenta pública, fuentes académicas, medios de prensa, bases de datos pública, etc.

Como señalan Szymoniak y Foks (2024), la actividad de OSINT debe seguir un lineamiento ético tanto en su modo de obtención como utilización de la misma. Las metodologías deben enmarcarse en las regulaciones y leyes correspondientes, y tener un fundamento en el porqué y el para qué.

La regulación interna determinará el alcance y los límites de los investigadores. No es lo mismo una red social cuya información se encuentre disponible a cualquier usuario que una que tenga restricciones para aquellos terceros que no lo permita. Se pueden hacer distinciones además en otro tipo de fuentes que pueden ser accesibles con un simple registro o aquellas que requieran un pago de servicio para su acceso. En principio, dependiendo el caso particular, ya dejaría de ser OSINT.

Respecto a las herramientas, hay cientos de software que facilitan la explotación de estas fuentes abiertas. Están los buscadores para todo lo indexado en la web, siendo Google el más conocido en Occidente, Baidu en China o Yandex en Rusia. Existen operadores para aplicar en estos motores de búsqueda para lograr mayor precisión y efectividad, ya sea incluyendo, excluyendo, filtrando o seleccionando. En el caso de Google se conocen como *Google Dorks.*

Vinculado a lo geográfico, se encuentran los mapas en línea que ofrecen los distintos proveedores con sus satélites. Muchos, además de la propia visualización satelital en la proyección MERCATOR, permiten acceder a imágenes o fotografías desde la ruta, lo que facilita la identificación detallada de inmuebles, caminos o terrenos. Entre los más conocidos se encuentran Google Maps, Bing Maps, Open Street Map, entre

otros. Hay decena de complementos que añaden funcionalidades de utilidad para el trabajo con mapas y son de suma utilidad para una investigación. Por ejemplo, hay aplicaciones que realizan el cálculo de la luz solar durante un horario determinado o el tiempo recorrido entre determinados puntos.

La búsqueda por imágenes es un instrumento para obtener más información como puede ser la identificación de una locación o un elemento. Están disponibles soluciones más desarrolladas para otros servicios, por ejemplo, la identificación de rostros.

En materia de conocimiento de infraestructura e información tecnológica, hay recursos web que brindan información de dominios, *IPs*, proveedores. Whois es de los más conocidos, pero hay numerosas opciones. Shodan.io es un buscador de dispositivos conectados a internet, revelando información pública de los mismos.

Las redes sociales (RR. SS.) son otra fuente de generación permanente de contenido en fuentes abiertas. Un número reducido de empresas concentra la mayor parte del mercado, y existen herramientas de monitoreo en tiempo real para el seguimiento de temas de interés o de seguridad nacional.

Se puede continuar listando otros tipos de herramientas utilizadas para la obtención de información de interés. No solo son de utilidad para agencias gubernamentales en búsqueda de actividades ilícitas o investigaciones penales en curso, sino también para causas nobles impulsadas por la sociedad civil, como búsquedas de personas desaparecidas. Por otro lado, también es una manera de las que se valen los criminales para recabar información con el fin de puntualizar ataques, técnica muy utilizada en ataques cibernéticos.

2.2. Teoría de grafos aplicada al análisis de datos

En el contexto del gran flujo de datos que puede generar una persona en sus actividades cotidianas, como telecomunicaciones, operaciones financieras, utilización de servicios digitales, rutas realizadas, entre otros, al pensarlo a una organización delictiva, los mismos crecerán exponencialmente. Luego de la etapa de obtención de la información, debe realizarse el proceso que implica la valoración, análisis e integración de la misma (Navarro Bonilla, 2004).

Aquí suscita interés la teoría de los grafos, una rama de la matemática que estudia la relación entre objetos a partir de grafos. Como expresan Constanzo *et al.* (2017), estos están conformados por un nodo que representan entidades y aristas que simbolizan conexiones de estos nodos. A modo práctico y de ejemplo, un nodo representa un individuo, una arista de llamada telefónica unida a otro nodo que representa otro

individuo. De esta manera, ante un determinado número de individuos y centenas de llamadas, podrían establecerse vinculaciones, patrones y estadísticas.

El mapa de grafos con sus nodos y aristas dará lugar a una red social, definida por Wasserman y Faust (1994) como estructura relacional de un grupo o sistema social más amplio que consiste en el patrón de las relaciones entre la colección de actores. A partir de allí es factible el análisis de redes sociales con base en conceptos como la intermediación, donde se identifica los nodos que se encuentran entre medio de otros y controlan el flujo de información o cohesión que permite identificar subgrupos interconectados entre sí. Del mismo modo pueden establecerse valoraciones numéricas sobre la base de la densidad de cada nodo, como la relevancia de este de acuerdo con la variable que pondere el analista.

Este tipo de herramientas como Maltego (que también tiene herramientas de OSINT), Gephi o Neo4j son de extrema utilidad para el procesamiento y análisis de grandes volúmenes de datos que con un tratamiento manual no podría realizarse.

En este apartado es menester mencionar la existencia de software de código abierto como privado diseñado para la visualización con grafos y trazabilidad de criptomonedas en tiempo real. Tal solución facilita el trabajo de los investigadores ante una metodología cada vez más utilizada por los delincuentes para recibir, transferir u ofuscar dinero ilícito beneficiándose en la parcial regulación y control del sector.

2.3. Sistemas de información geográfica

La utilización de SIG para el análisis delictual y criminal es una forma para el aprovechamiento y conocimiento de los datos geoespaciales referidos a hechos como actividades. Los mismos se conforman de puntos, líneas y polígonos que contienen atributos donde pueden encontrarse más datos además de los espaciales. A modo de ejemplo, otros datos que pueden procesarse son el tipo de delito, arma utilizada, elementos robados, etc. (Ratcliffe, 2010).

A diferencia de las herramientas en línea como Google Maps o Bing Maps; los SIG permiten realizar un análisis más sofisticado para la prevención policial o ante hechos específicos. Son muy utilizados para determinar áreas de alta concentración delictual (*hotspots*), análisis del delito en el tiempo y sus variaciones, y la detección de patrones espaciales.

Por ejemplo, si se investiga una banda dedicada al robo de automóviles de alta gama, con el uso de SIG podrían determinarse zonas de mayor incidencia y posteriormente evaluar las posibles rutas de escape y la georreferenciación de los desarmaderos más cercanos. De esa manera se puede reorientar la estrategia

investigativa en las tareas en el terreno como patrullajes focalizados o la búsqueda de cámaras.

QGIS es un software en código abierto con alta flexibilidad, que permite la manipulación con complementos y *scripts*. Por su parte ArcGIS es una solución privada que ofrece herramientas y complementos para el análisis espacial, y algunos específicos en seguridad y mapeo del delito.

2.4. Forensia digital

Se estima que una persona utiliza cinco dispositivos tecnológicos en su vida cotidiana. El más utilizado es el dispositivo móvil, seguido por notebooks o computadoras de escritorio, televisores inteligentes, relojes inteligentes, etc. Ya previo al año 2005 con el advenimiento de internet, se empezaron a desarrollar actividades ilícitas como *malware* o pornografía infantil, por lo que las fuerzas de la ley debieron profesionalizar sus laboratorios forenses (Pollit, 2010). En este contexto empieza a tomar fuerza la informática forense, cuyo objetivo es adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional (FBI).

El tratamiento del tipo de dispositivo, y a su vez de marcas y modelos, varía en las herramientas a utilizarse, como la especialidad del perito. La extracción de datos en dispositivos móviles presenta distintos desafíos que en computadoras desde el punto de vista tecnológico y metodológico. Además, el crecimiento del Internet de las cosas (IoT, por sus siglas en inglés) amplía el espectro del análisis forense.

En el caso de los móviles, la robustez de los sistemas en sus versiones recientes de Android y Iphone ha hecho que el software de código libre u obsoleto no tenga éxito en su propósito. Sin embargo, los procesos de extracción se han simplificado con soluciones empresariales como XRY de MSAB o UFED de Cellebriti, que ofrecen además complementos para el análisis de datos mediante la categorización, líneas de tiempo, herramientas de visualización e integración de dos o más dispositivos (Sutikno y Busthomi, 2024).

La importancia de la información obtenida es de alto valor para los investigadores, que pueden disponer de información relativa a mensajería, ubicaciones, archivos multimedia, y demás datos que pueda obtener el software.

Por su parte, el análisis forense en computadoras lleva consigo otras herramientas y metodologías donde la recolección de evidencias dependerá de factores como los sistemas de almacenamiento, cifrados, volatilidad de los datos, tipos de archivos, archivos borrados, registros en el sistema, entre otros (Almeida Romo, 2011).

3. Desafíos y conclusiones

Como se ha descripto, una investigación criminal en profundidad en cualquiera de sus etapas puede generar una gran cantidad de datos; tanto en una fase preliminar, donde pueden valerse de herramientas de fuentes abiertas, como en una fase investigativa más profunda, en donde los magistrados dan lugar judicialmente a la recolección de más información relativa a la causa. En casos donde las investigaciones tienen éxito y son secuestrados elementos de interés tales como móviles, la información continúa incrementándose.

En ese sentido, se plantean distintos desafíos que deben hacer frente los decisores de políticas públicas en consonancia con las instituciones dedicadas a la seguridad pública, independientemente de su nivel y jurisdicción de actuación.

En primer lugar, se debe tener presente la escasez de recursos humanos y tecnológicos. La profesionalización de agentes capaz de realizar tareas analíticas es sumamente necesaria, en consecuencia a la complejidad y grandes volúmenes de datos. Del mismo modo, es necesario entender que la criminalidad se va tecnificando en su *modus operandi* y en el uso de la tecnología.

En el caso del despliegue de los lugares de trabajo en donde se realiza la manipulación y tratamiento de datos, debe poseerse una infraestructura de hardware moderna y actualizada, y redes de trabajo segmentadas que garanticen la seguridad de la información. Se suma también, en el caso de elementos secuestrados, la necesidad de lineamientos y protocolos enmarcados en las correspondientes regulaciones para su seguro resguardo en una locación física adecuada.

El software requerido en ocasiones suele ser de carácter pago a través del otorgamiento de licencias onerosas, algunos de las cuales ofrecen versiones intermedias y premium, y complementos adicionales para funcionalidades específicas.

Asimismo, el exceso de datos requiere de estrategias de *triage* para economizar el tiempo y los recursos disponibles. Los analistas deben depurar, filtrar y clasificar la información relevante, como también basarse en soluciones automatizadas que permitan prescindir del trabajo manual en su mayor medida.

Aunque los crímenes en el mundo virtual datan de años, continúa siendo un entorno poco conocido e impredecible, lo que supone un reto para los Estados. Estos delitos y actividades presentan una real amenaza a la soberanía y finanzas de los Gobiernos, así como empresas y ciudadanos

En materia regulatoria, todo Gobierno debe trabajar con base en los marcos legales locales e internacionales. Se debe cumplir los derechos y garantías, así como la correcta

manipulación de los datos y sus obligaciones correspondientes. La armonización con el derecho internacional es una misión que deben impulsar los Gobiernos centrales para aplicar mejoras en sus estándares y respuestas ante los delitos transnacionales. Un ejemplo de ello es la Convención de Budapest sobre Ciberdelincuencia de 2004 y ampliada en el 2022 con protocolo adicional para la obtención de evidencia digital más allá de las fronteras.

Finalmente, todos los actores deben promover la cooperación intraestatal en sus diferentes niveles de gobierno, como a nivel interestatal, fomentando el intercambio de información y división de trabajo según especialidad de la institución. De la misma manera, es importante explorar instancias similares con el sector privado, que en ciertos casos disponen de tecnología y recursos superadores.

En conclusión, los delitos de carácter transnacional requieren de un abordaje mancomunado para lograr la desarticulación de las cadenas delictivas en sus distintos eslabones. Por ello, la capacidad de los Estados en impulsar estructuras adaptativas, flexibles e innovadoras será clave para garantizar el cumplimiento de sus objetivos y responsabilidades.

Referencias bibliográficas

Almeida Romo, O. R. (2011). *Metodología para la implementación de informática en sistemas operativos Windows y Linux.* Tesis de grado. UTN. https://repositorio.utn.edu.ec/bitstream/123456789/539/8/04%20ISC%20157%20CAPITULO%20III.pdf

Block. L. (2024). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95-109. https://doi.org/10.1080/16161262.2023.2224091

Constanzo, B., Lamperti S., Lasia S., Podestá, A., Cistoldi, P. y Di Iorio, A. H. (2017). *El análisis automático de datos, su aporte a la investigación criminal*. InFo-Lab. (Universidad FASTA, Ministerio Público de la Provincia de Buenos Aires, Municipalidad de General Pueyrredón).

Global Initiative Against Transnational Organized Crime. (2023). Global organized crime index 2023. Geneva, Switzerland: The Global Initiative Against Transnational Organized Crime.

Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton University Press.

Navarro Bonilla, D. (2004). El ciclo de inteligencia y sus límites. *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, (48), 51–66.

Pollitt, M. (2010). A History of Digital Forensics. En Chow, K. P., Shenoi, S. (Eds.). *Advances in Digital Forensics VI. DigitalForensics. IFIP Advances in Information and Communication*

Technology, vol. 337. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15506-2_1

Ratcliffe, J. (2010). Crime mapping: Spatial and temporal challenges. En A. Piquero & D. Weisburd (Eds.). *Handbook of quantitative criminology* (pp. 5–24). Springer. https://doi.org/10.1007/978-0-387-77650-7_2

Reyes Pozo, V. V. (2024). *Análisis de redes sociales para mejorar la eficiencia en la persecución penal* [Tesis de grado, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Departamento de Ingeniería Industrial].

Sutikno, T., & Busthomi, I. (2024). Capabilities of Cellebrite Universal Forensics Extraction Device in mobile device forensics. *Computer Science and Information Technologies,* 5(3), 254–264. https://doi.org/10.11591/csit.v5i3.pp254-264

Szymoniak, S., & Foks, K. (2024). Open Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*, 18(3), 123–139. https://doi.org/10.12913/22998624/186036

Ugarte, J. M. (2024) La inteligencia criminal: concepto, implementación, experiencias comparadas. *Revista Política y Estratégica* (143), 69-110. https://doi.org/10.26797/rpye.vi143.1082

Wahler, S. P., Larrea, M. L., & Martínez, D. C. (2022). *Una herramienta de análisis y visualización de redes sociales para la identificación de bandas delictivas*. Simposio Informático del Estado.

Wasserman, S., & Faust, K. (1994). Social network data. En *Social network analysis: Methods and applications* (pp. 17–94). Cambridge University Press. https://doi.org/10.1017/CBO9780511815478