ICCSI

INICIATIVA CIUDADANA PARA
EL CONTROL DEL SISTEMA
DE INTELIGENCIA

Acerca de la inteligencia criminal en Argentina

Apuntes para su discusión

CELS centro de estudios legales y sociales
ILSED Instituto Latinoamericano de Seguridad y Democracia
Fundación Vía Libre

Créditos

Dirección
Fundación Vía Libre (FVL)
Beatriz Busaniche

Equipo de redacción
Instituto Latinoamericano de Seguridad y Democracia (ILSED)

Coordinación
Tamara Peñalver

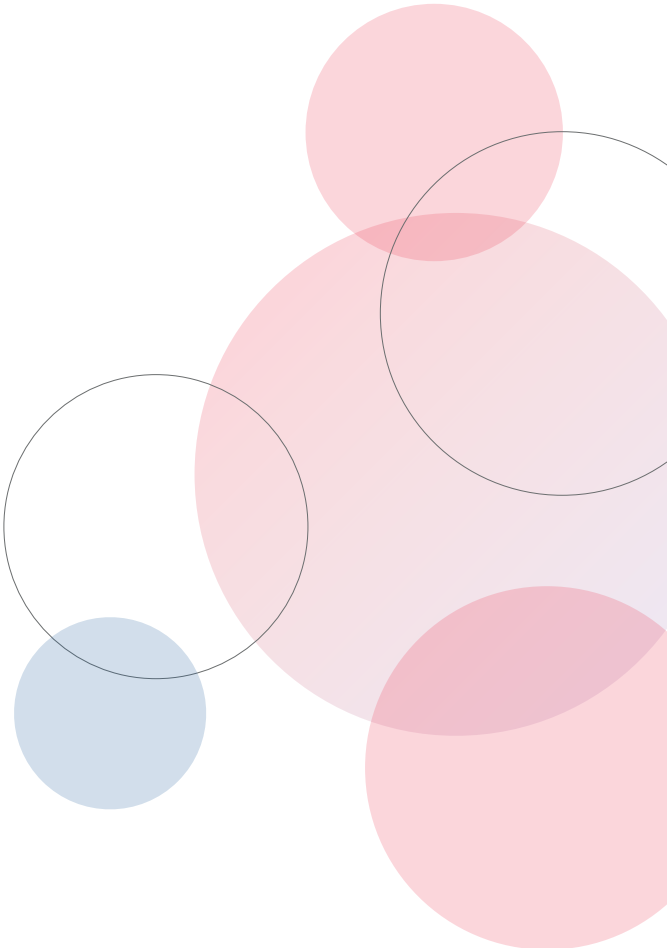
Investigadoras/es
Ana Clara Montañez
Bárbara Sosa
Joaquín Chesini

Colaboradoras/es
CELS - Centro de Estudios Legales y Sociales
Luciano Coco Pastrana
Margarita Trovato
Manuel Tufró

Asesoramiento
Alberto Binder
Enrique Chaparro
Paula Litvachky

Diseño
Carolina Marcucci

Esta publicación fue realizada
con el apoyo de Luminate.



Índice

Presentación y agradecimientos

Una de las principales deudas de la democracia en Argentina es la necesidad de regular en forma precisa la actividad de inteligencia estatal dentro de los distintos ámbitos institucionales en los que es necesario su despliegue. En este sentido, aún se encuentra pendiente un debate profundo en torno a generar las condiciones legales e institucionales propicias para el desarrollo de la inteligencia, en pos de mejorar la eficacia de las decisiones de gobierno, bajo el resguardo de los derechos que pueden estar en riesgo frente a dicha actividad.

La Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI)[1] ha trabajado desde su nacimiento en esta línea, promoviendo reformas desde la sociedad civil hacia las esferas pertinentes del sector político, en miras de lograr la democratización de una actividad que se ha desarrollado, en reiteradas ocasiones, por fuera de los márgenes de la constitucionalidad.

Las ambigüedades y falta de rigor en relación a las conceptualizaciones y las regulaciones sobre lo que es la actividad de inteligencia y sus objetivos en concreto, han profundizado la falta de control y su utilización con fines espurios desde diversas instituciones estatales. Por ello, es indispensable refundar su marco conceptual y dar paso a un nuevo modelo de práctica de la inteligencia estatal con impacto en sus variantes, como lo son la inteligencia nacional, criminal y militar.

Este documento ha sido realizado con el objetivo de seguir impulsando el desarrollo de un mejor sistema de inteligencia, generando materiales de consulta para las transformaciones que serán necesarias sobre la que, hoy en día, es una actividad indispensable para mejorar la calidad de las decisiones que deben tomar los Estados frente a los desafíos que enfrentan las sociedades globalizadas.

En esta oportunidad, nos enfocaremos en la inteligencia criminal y haremos especial hincapié en desarrollar teóricamente algunos puntos neurálgicos de esta actividad de cara a los recientes sucesos que han motivado su instalación en la agenda pública.

No pretendemos agotar aquí las discusiones ni abarcar todos sus aspectos, sino establecer algunos ejes que consideramos indispensables para sentar las bases de los debates que vendrán, dadas las vacancias que existen actualmente sobre ella en Argentina.

1. La Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI) es un espacio destinado al seguimiento, impulso y promoción del funcionamiento efectivo de los mecanismos de control sobre el sistema de inteligencia de nuestro país. Representa una respuesta de la sociedad civil a la necesidad de construir un espacio comprometido con la democratización de los organismos que hacen inteligencia, en particular, a través del impulso de políticas destinadas a mejorar los controles internos y externos del sistema para el buen funcionamiento del Estado de derecho y las instituciones democráticas. Más información disponible en el siguiente link. Última consulta: 16 de agosto del 2021.

Agradecemos el apoyo a la agencia Luminate[2], que ha contribuido con la producción de este documento, como con los diversos materiales y actividades de capacitación e incidencia que hemos realizado en relación a la divulgación del conocimiento e ideas vinculadas a la temática de inteligencia.

También agradecemos a Alberto Binder, Enrique Chaparro y Paula Litvachky por los aportes que han realizado para el desarrollo de las ideas que aquí se plasman[3]. Esperamos que sean de utilidad para detectar los puntos de partida y necesidades hacia el futuro.

¿Por qué decidimos realizar esta publicación?

La motivación para el desarrollo de esta publicación tiene su origen y contexto en dos políticas impulsadas en nuestro país durante el 2020.

En primer lugar, se gestó un nuevo debate para reformar la Ley de Inteligencia Nacional, como correlato de la intervención de la Agencia Federal de Inteligencia (AFI). En dicho contexto, integrantes de la ICCSI formaron parte del Consejo Consultivo de la intervención de la AFI y elaboraron, en conjunto con otras personas, un proyecto de ley que parte de una ruptura conceptual y organizacional respecto de la actual Ley 25.250 –reformada por la Ley 27.126 y el Decreto 214/2020 .

En este sentido, el anteproyecto de ley[4] establece conceptos, alcances y límites claros a la actividad de inteligencia nacional y separa las funciones de la AFI del resto de las organizaciones encargadas de realizar otros tipos de inteligencia, como lo son la criminal y la militar, algo que desde la academia se viene promoviendo.

De esta forma, propone romper la lógica de "comunidad de inteligencia" que ha facilitado vinculaciones ilegales entre agentes de inteligencia y otros actores, como policías y funcionarios/as judiciales –y también vale mencionar periodistas y políticos/as–, para pasar a un "sistema de coordinación intergubernamental", que parte de la base de regular funciones precisas dentro de cada organización encargada de cada tipo de inteligencia y, en consecuencia, favorecer al desarrollo de los niveles de control interno y externo sobre el personal y sus responsabilidades.

2. Luminate. Página web oficial en el siguiente link. Cabe aclarar que las ideas de este documento no representan las posturas de la fundación Luminate respecto al tema. Última consulta: 16 de agosto del 2021.

3. Destacamos que desde ILSED, FVL y el CELS hemos trabajado y reflexionado en torno a la bibliografía y normativa existente, nacional e internacional y hemos arribado a la conclusión preliminar de que no existe, en la actualidad, un desarrollo teórico consolidado en materia de inteligencia criminal y que restan amplias discusiones para construir un marco conceptual claro y acabado. Por estos motivos, el documento pretende ser un primer acercamiento a los debates y consideramos necesario continuar con el proceso de consolidación de ideas y bases teórico-prácticas. No es tampoco una sorpresa esta primera conclusión, ya que la inteligencia criminal, en tanto actividad estatal, atraviesa diversas instancias y discusiones sumamente vinculadas a más de una política pública, como lo son la seguridad, la política criminal y la judicial y, a su vez, a diversas aristas que van desde la protección de datos, la seguridad informática y las nuevas tecnologías, sumamente inexploradas a nivel local.

4. El anteproyecto de ley fue presentado a la intervención de la AFI en miras de que sea discutido dentro del Congreso de la Nación. El anteproyecto también fue presentado a la comunidad académica. Para conocerlo ingresar al siguiente link. Última consulta: 16 de agosto del 2021. Link

Así, la propuesta de reforma impacta directamente en las necesidades regulatorias de la inteligencia criminal, por lo que es preciso abordarlas y discutirlas con el fin de establecer algunas de las pautas para su desarrollo normativo y, por supuesto, su transformación al interior de las prácticas institucionales. El anteproyecto de ley cristalizó los vacíos en torno a este tema, y más temprano que tarde habrá que discutir los ejes centrales de la actividad de inteligencia criminal.

En segundo lugar, el Ministerio de Seguridad de la Nación puso en funcionamiento un protocolo que denominó *Prevención policial del delito con uso de fuentes digitales abiertas*[5] –llamado coloquialmente protocolo de *ciberpatrullaje*–, destinado a instruir a las fuerzas de seguridad federales para la prevención, en el espacio digital, de diversos tipos de criminalidades, que entendieron podrían desarrollarse como consecuencia de la pandemia Covid-19 y la emergencia sanitaria declarada en Argentina[6].

Dicho protocolo se estableció, en principio, para atender el surgimiento de posibles delitos vinculados a la pandemia y al notorio desplazamiento de la criminalidad hacia las esferas digitales al comienzo de las disposiciones de Aislamiento Preventivo y Social Obligatorio (ASPO). Sin embargo, presentaba un carácter difuso en torno al tipo de actividad que regulaba, al modo en que iba a desarrollarse y a los problemas criminales sobre los que tendría competencia.

Entre otras cosas, lo que desde el Ministerio de Seguridad de la Nación se planteaba como una actividad de mera prevención policial, para la ICCSI constituía –y constituye– una actividad de inteligencia criminal cuyas fuentes de información se caracterizan por ser digitales. Esto, hasta el día de hoy, carece de legislación regulatoria.

Entonces, las posturas diversas en torno al protocolo evidenciaron la necesidad de precisar categorías y delimitar las prácticas que deben ser reguladas y las que deben ser prohibidas. Sin dudas, la novedad del tema, la falta de naturalización de la actividad y su oquedad estructural, traslucieron en tiempo real las dificultades que enrolan a la inteligencia criminal en la era digital.

Ahora bien, más allá de los problemas que presentaba el protocolo, permitió reinstalar el debate acerca de la inteligencia criminal en específico y la premura de establecer un marco legal particular, que acompañe las actuales discusiones, los avances de las nuevas tecnologías para la recolección de información y las transformaciones de la criminalidad en sus diversas manifestaciones.

En función de todo lo anterior, es que hemos trabajado en la presente publicación para aproximarnos a las bases y a los problemas que podrían ser tenidos en consideración al momento de debatir sobre las regulaciones pertinentes de

5. Resolución del Ministerio de Seguridad de la Nación Nº 144/2020. Boletín Oficial. Fecha: 31 de mayo del 2020. Disponible en el siguiente link. Última consulta: 16 de agosto del 2021.

6. Ley 27541. Disponible en el siguiente link. Última consulta: 16 de agosto del 2021.

la inteligencia criminal, la cual debería estar destinada a la planificación de estrategias y acciones de seguridad pública, la política criminal y la persecución penal, dejando de lado posibles prácticas irregulares y poco transparentes.

En el capítulo 1, hacemos hincapié en el desarrollo de los ejes centrales que actualmente se encuentran en discusión vinculados a la actividad de inteligencia criminal. Esto es, su definición conceptual y objetivos, las organizaciones productoras y requirentes (clientes/clientas), las decisiones que la involucran y los conceptos asociados con los que suele confundirse y que son necesarios discernir.

En el capítulo 2, mencionamos las nociones básicas acerca de las limitaciones que posee la actividad de inteligencia criminal. Es decir, cuáles son los principios rectores de la actividad que deben ser puestos en práctica al momento de su desarrollo y las funciones que deben cumplir en forma pragmática para garantizar el respeto de los derechos fundamentales.

En el capítulo 3, ofrecemos una propuesta metodológica para el ciclo de inteligencia criminal, conformado por diversas dimensiones con asuntos y problemáticas concretas que deben ser atendidas en cada una, y que son claves para la legalidad y eficacia de la actividad.

En el capítulo 4, nos focalizamos en las discusiones actuales sobre la inteligencia criminal en relación a fuentes abiertas, tomando como referencia el protocolo de *Prevención policial del delito con uso de fuentes digitales abiertas* del Ministerio de Seguridad de la Nación y su impacto para repensar la regulación de este tipo de actividad en la coyuntura de nuestro país.

Para finalizar, detallamos algunas de las necesidades de cara al futuro para regular una inteligencia criminal como actividad estatal que respete las garantías para la toma decisiones relevantes y que, a su vez, procure mejorar la calidad de las decisiones en materia de criminalidad y violencias.

1.

La inteligencia criminal: aproximaciones para su definición y alcances

La inteligencia criminal: aproximaciones para su definición y alcances

Necesidad de una nueva conceptualización

Establecer una definición en torno a la inteligencia estatal es un desafío complejo de abordar, debido a que existen debates que aún se encuentran abiertos. Es decir, pese a la amplia gama de definiciones en la literatura, donde según quién escriba se destaca un elemento diferente de esta actividad, ninguno de los esquemas conceptuales es suficiente para abarcar todo lo que la inteligencia representa en la práctica, en términos de organizaciones responsables, alcances, límites y acciones[7]. Por lo tanto, la consolidación teórica sobre ella en nuestro país se torna urgente y necesaria para establecer un lenguaje común que permita mejorar las prácticas actuales del funcionamiento del sistema de inteligencia estatal.

Para contribuir con ello, consideraremos aquí a la inteligencia estatal como una actividad orientada a la producción de información *accionable*[8] para la toma de decisiones sobre problemas que deben ser atendidos por el Estado, desarrollada a través de un ciclo propio de información[9] y desplegada conforme a determinadas restricciones de orden constitucional, legal y reglamentario. Debe servir de apoyo a la toma de decisiones de los organismos del Estado encargados de la elaboración, formulación, planificación, implementación y evaluación de diversas políticas, estrategias y acciones de orden nacional e internacional.

Asimismo, dentro de la inteligencia estatal, en una relación de género y especie, se encuentra la inteligencia criminal sobre la cual la discusión teórica es más escueta y diseminada, generando consecuencias en su escasa

7. El concepto de inteligencia ha sido desarrollado como producto, proceso, organización, conocimiento, actividad, entre otros. Para hacer una breve referencia, diremos que algunos autores como Richelson, la conciben como un producto final de un proceso integral, es decir, el énfasis se encuentra en el reporte -resultado de un proceso de análisis de la información- que permitiría tomar decisiones de manera inteligente (2008, p. 2). Mientras que, otros autores como Lowental -citado por Ugarte-, la comprenden como proceso, centrándose en lo que se conoce como ciclo de inteligencia, integrado por una serie de pasos, jerárquicamente ordenados y rigurosamente cumplidos para producir información a ser utilizada en la posterior toma de decisiones estatales (2001, p. 41). Por otro lado, hay quienes la entienden como organización y enfatizan en el carácter sistémico de la disciplina en cuanto a las organizaciones que forman parte de ella (Ugarte, 2001, p. 52). Sumado a esto, la inteligencia también es entendida como conocimiento y suelen hacer alusión a ella como conocimiento especializado en la protección de los intereses del Estado-Nación (Ugarte, 2001, p. 42). Desde esta perspectiva, la inteligencia es el producto de la evaluación aplicada sobre la información, que deviene en inteligencia como conocimiento en un estadio superior a ser utilizado como orientador de decisiones (Criminal inteligencie manual for managers, 2011, p. 1). Finalmente, quienes conciben a la inteligencia como actividad, refieren a la acción misma frente a un problema, amenaza u objetivo (Ugarte, 2001, p. 50). Esta es una postura que se focaliza en la perspectiva práctica de la inteligencia.

8. Entendemos por accionable aquella información que da lugar a la acción, en este caso, a la toma de decisiones propias de la inteligencia. La información consiste en la elaboración de hipótesis e interpretaciones que permiten orientar la política.

9. Denominado comúnmente como ciclo de inteligencia.

regulación a nivel local. En este sentido, la Ley de Inteligencia Nacional 25.520[10] brinda una definición poco clara para la práctica de la inteligencia criminal, situación no resuelta tampoco a partir de la nueva doctrina de inteligencia nacional –Decreto 1.311/2015 y anexos–.

Por el momento, a los fines de realizar una aproximación para una nueva conceptualización entenderemos aquí a la inteligencia criminal como aquella actividad orientada a la producción de información accionable para la toma de decisiones, en un espectro amplio, que abarca desde los asuntos de seguridad pública y de política criminal hasta la persecución penal en un caso en particular. Es desplegada mediante un ciclo de información, integrado por distintas dimensiones que lo ordenan, y tiene como productores y/o clientes a los ministerios de seguridad, a las fuerzas policiales, a los ministerios públicos fiscales y a las fiscalías. Asimismo, en cada ámbito organizacional en que se desarrolla debe tener limitaciones y autorizaciones particulares en función de cada una de las dimensiones del ciclo de inteligencia criminal que más adelante veremos.

Cabe señalar que esta definición pretende hacerse cargo en forma incipiente de diversas cuestiones que hacen a la actividad: quiénes pueden desplegarla y quiénes pueden ser clientes/as; sobre qué asuntos es posible su utilización; y, cómo debe ser aplicada teniendo en cuenta habilitaciones y restricciones.

Estos tres puntos son los que debemos discutir hacia el futuro para delinear una definición más robusta y el conjunto de prácticas que involucran a la inteligencia criminal de forma acabada. De esta manera, podremos colaborar para que el Estado tome decisiones efectivas de cara a los problemas y conflictos criminales que debe afrontar frente a los cambios sociales y, a su vez, apoye las actualizaciones que deben transitar las organizaciones estatales como consecuencia de ello.

Esto es, la inteligencia criminal de ahora en adelante debería asumir un rol trascendental en analizar las nuevas manifestaciones de la criminalidad y en la selección de herramientas modernas para el diseño de la seguridad y de la política criminal, haciéndose cargo también del uso de tecnologías emergentes inexploradas en nuestro país.

10. La Ley de Inteligencia Nacional refiere, además, a la inteligencia nacional y a la estratégica militar. Por lo que se entiende que el sistema de inteligencia argentino actualmente pretende regular la inteligencia nacional, la militar y la criminal, dejando por fuera otro tipo de inteligencias. No obstante, las conceptualizaciones de cada una de ellas se encuentran en crisis bajo la necesidad de generar reformas tanto teóricas como institucionales de cara a los nuevos problemas estatales. De esta manera, se ha comenzado a trabajar por la inteligencia nacional sobre la que el Consejo Consultivo de la AFI ha generado una nueva definición entendiéndose como aquella encargada de generar conocimiento referido a los hechos y riesgos que puedan afectar los bienes, intereses y actividades esenciales para el desarrollo integral del país, con el objetivo de proteger la soberanía nacional, preservar el orden constitucional, orientar sus relaciones internacionales y planificar su inserción en el contexto mundial (proyecto de ley elaborado por Consejo Consultivo de la AFI, 2020, art. 2. inc. 1. p. 6). Resta, entonces, comenzar a discutir las definiciones actuales de inteligencia criminal y militar, en miras de que las sociedades y sus problemáticas evolucionen más rápido que las legislaciones y prácticas institucionales.

Obviar estos ejes a lo largo del tiempo ha llevado a acciones improductivas, ineficaces y poco claras, que trajeron consecuencias negativas para el despliegue de la actividad, entre ellas, que no exista claridad en quiénes son responsables de ejecutarla o bien quién debe controlar cada una de las acciones, aspectos básicos de cualquier asunto estatal[11].

Delineando sus ámbitos de aplicación

La inteligencia criminal en tanto actividad estatal debe servir, como hemos dicho, para la producción de conocimiento para la toma de decisiones en materia de políticas públicas centrales: la seguridad y la política criminal (y dentro de esta última, la persecución penal). Ambas políticas públicas se abocan al abordaje de la criminalidad y las violencias, a partir de la utilización de diversos recursos estatales. Podemos decir que son las políticas públicas que por excelencia deben articularse a los fines de controlar, reducir, transformar y/o extinguir los problemas públicos criminales.

La seguridad pública es aquella destinada a intervenir sobre la criminalidad y las violencias a partir del uso de diversos recursos para su prevención, disuasión y conjuración como son, por ejemplo, las fuerzas policiales y su sistema de patrullaje, las alarmas vecinales, las policías comunales, la instalación de cámaras de videovigilancia, las distintas estrategias de participación comunitaria en asuntos de seguridad, entre otras alternativas que actualmente se están explorando para salir de las tradicionales acciones policiales.

La política criminal, por su parte, es aquella que administra los recursos más violentos del Estado –las fiscalías, las policías de investigaciones[12] y las cárceles– para intervenir en la criminalidad y las violencias (Binder, 2011, p. 288). Es decir, la política criminal, entre otras cuestiones, es la encargada de diseñar el despliegue de investigaciones de diversa índole, conforme a las regulaciones procesales penales particulares, como lo son las genéricas, las preliminares o las formalizadas, con el objetivo de tener un impacto favorable en términos de fenómenos criminales. Cada tipo de investigación estará destinada a objetivos concretos, sea conocer el desarrollo de un problema público criminal (genéricas) o una determinada actividad delictiva y sus supuestos responsables

11. Esta circunstancia fue remarcada por el Consejo Consultivo de la AFI en la exposición de motivos del Anteproyecto de la Ley de Inteligencia Nacional, al momento de señalarse la necesidad de abandonar el esquema de "comunidad de inteligencia" para dar paso al modelo de articulación entre agencias responsables de la inteligencia criminal, nacional y militar.

12. En nuestro país tenemos otra deuda pendiente: la creación de policías especializadas en investigaciones que trabajen en forma directa y coordinada con los ministerios públicos fiscales y fiscalías. La reforma en materia policial se torna imprescindible para profesionalizar los sistemas investigativos en Argentina. Actualmente las fuerzas policiales poseen escasa especialidad para trabajar en investigaciones, lo cual distorsiona los resultados que podrían obtenerse en términos de eficacia y eficiencia.

(preliminares) o bien la asignación de responsabilidades penales en concreto frente a la judicatura con el fin de solicitar condenas y/o alternativas al proceso penal (formalizadas)[13].

De esta manera, las agencias productoras y/o clientas de la inteligencia criminal, como hemos mencionado, deberían ser los ministerios de seguridad, las fuerzas policiales de prevención y de investigación y los ministerios públicos fiscales (en adelante MP) y fiscalías, en sus diversos niveles de orden jerárquicos y funciones, según la decisión que deba tomarse y el tipo de conocimiento que deba producirse en consecuencia.

Las decisiones y/u objetivos que podría apoyar la actividad de inteligencia criminal se encuentran en diversos niveles decisionales vinculados a estrategias generales, operacionales y/o tácticas. Esto es, permite producir conocimiento para la toma de decisiones en diversos planos de mando jerárquico, por ejemplo:

→ Diseño de planes de seguridad y de política criminal sobre fenómenos criminales a largo, corto y mediano plazo que, a partir del conocimiento del problema en profundidad, sus causas, evolución, estructura, manifestaciones y segmentos, permitan orientar los recursos, estrategias y acciones.

→ Líneas de investigación orientativas en el contexto de la persecución penal aplicada en investigaciones genéricas, preliminares y/o formalizadas, según la que se esté desplegando, y la decisión que allí sea necesario tomar.

→ Producción de evidencia en el contexto de una causa penal con el objetivo de avanzar hacia la resolución del caso, conforme a las reglas del debido proceso.

→ Distribución, utilización y maximización de los recursos institucionales (presupuestarios, recursos humanos, edilicios, tecnológicos) y su permanente evaluación para determinar su eficacia y eficiencia.

→ La puesta en marcha de alertas tempranas que permitan detectar anticipadamente un suceso delictivo y desplegar los recursos en pos de su neutralización.

→ Articulación de políticas, estrategias y acciones con agencias estatales vinculadas al problema público criminal que se quiere abordar con el fin de generar herramientas preventivas y reactivas de impacto.

13. Estas categorías pueden variar de denominación según la legislación procesal penal. Solo pretendemos marcar la distinción entre aquellas investigaciones que no han sido formalizadas ante la judicatura y aquellas que sí, ya que poseen objetivos distintos y están sujetas a disímiles limitaciones y habilitaciones. Sobre las primeras, en general, se hará referencia a las investigaciones genéricas como aquellas destinadas a conocer un fenómeno criminal y sus modalidades, sin autor/a indentificado/a, y a las preliminares como aquellas que se impulsan de oficio a partir de indicios sobre la comisión de un delito con el fin de identificar las circunstancias y sus responsables. En relación a las segundas, las judicializadas, se suele hacer referencia a aquellas investigaciones que se presentan ante la judicatura mediante la formalización de cargos o imputaciones contra personas en concreto, ya individualizadas. Cabe decir que presentan más distinciones sobre las cuales no profundizaremos en esta ocasión. Hemos tomado como referencia lo regulado en la ley 27063 y sus modificatorias.

→ Diseño de la estructura organizacional al interior de los ministerios de seguridad, las fuerzas policiales, los ministerios públicos y las fiscalías en miras de hacer frente a las problemáticas de las que deben ocuparse.

Por supuesto, estos son algunos ejemplos, pero la inteligencia criminal puede cumplir con otros objetivos institucionales o apoyar diversas decisiones que varían en función de las necesidades existentes en un tiempo y espacio determinado, las cuales son complejas de describir, adelantar y/o prever en forma acabada en este documento.

Lo que aquí queremos señalar es que la inteligencia criminal, en lo que respecta a la seguridad pública, la política criminal y la persecución penal, tendrá diversos niveles de orientación decisionales, que van desde la planificación en términos macro hasta las acciones concretas a niveles micro. Es decir, pretendemos mostrar un abanico de aplicación dentro del cual la inteligencia criminal cobra sentido y no prescribir todas y cada una de las oportunidades en que puede ser útil.

En síntesis, cada nivel de conducción organizacional –alto, medio e inferior– requerirá de conocimientos específicos en función, no solo de su dimensión de actuación, sino de la visión y el alcance que tiene de los problemas y asuntos sobre los que debe tomar decisiones. La actividad de inteligencia dentro de las organizaciones responsables debe intentar responder a las preguntas: ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué? y ¿para qué? La inteligencia en sí permite tomar decisiones con mayor calidad, dada la producción de información como respaldo de las mismas. Esa es su característica fundamental.

Algunas aclaraciones. La inclusión de los MP y las fiscalías como actores productores y/o clientes de inteligencia criminal requiere algunas precisiones, ya que no es habitual que se los nombre en la producción teórica sobre la actividad. Los MP se han transformado, a partir de las reformas procesales penales, en actores fundamentales para el abordaje de la criminalidad y las violencias. En sintonía, han adquirido nuevas funcionalidades, diseños organizacionales y herramientas para fomentar su profesionalización y ampliar su proactividad.

Las investigaciones genéricas y preliminares (aquellas que no han sido formalizadas judicialmente) constituyen herramientas fundamentales para la planificación de la política criminal y la persecución penal, por ende, para la producción de conocimiento que avale las decisiones vinculadas. De esta forma, la actividad de inteligencia criminal se podrá desarrollar en el contexto de este tipo de investigaciones ya que son orientadoras de acciones para la política criminal.

Ahora bien, si la información producida, sea en el contexto de investigaciones genéricas o preliminares, se quiere utilizar como evidencia para asignar responsabilidades penales, en cualquier instancia, deberá atravesar las exigencias del debido proceso penal. Además, siempre que la utilización de una técnica

de recolección de información en su despliegue pueda generar algún tipo de lesión a un derecho constitucional deberá requerir de la autorización judicial correspondiente.

Cabe mencionar en particular que se ha regulado que, en las investigaciones genéricas, se puede solicitar y producir información tendiente a la identificación de fenómenos criminales que orienten la constatación de hipótesis delictivas a partir de una o varias investigaciones preliminares[14]. Es decir, no están naturalmente destinadas a la identificación particular de personas y acciones típicas para su juzgamiento, como sí lo están las preliminares y las formalizadas. Pues las investigaciones genéricas se encuentran focalizadas en el conocimiento del problema y sus segmentos, manifestaciones y regularidades, para proyectar su intervención desde diversas aristas. Ello deja a la vista que las definiciones de inteligencia criminal y de investigaciones genéricas ingresan en un terreno gris que habrá que esclarecer.

Por su parte, la inteligencia criminal también puede ser desplegada en el marco de investigaciones formalizadas, para orientar líneas de investigación o la producción de evidencia pertinente. La posibilidad de utilizar dicho conocimiento también deberá estar ajustada a las regulaciones del debido proceso penal y las garantías constitucionales.

La formalización de una investigación hace referencia a la formulación de cargos ante la administración de justicia penal –judicatura– contra determinadas personas que se presuponen como posibles autoras del hecho investigado. Aquí, inteligencia criminal e investigación penal adquieren mayor distinción conceptual en tanto persiguen objetivos diferentes y están sujetas a reglas diferentes.

Conceptos asociados

Como hemos mencionado, la inteligencia criminal en la región se encuentra actualmente en discusión, tanto en términos normativos como en sus prácticas profesionales. Producto de este proceso en construcción, se suele confundir la inteligencia criminal con la investigación penal, con las técnicas de recolección de la información secretas y con el análisis criminal, lo cual genera muchas inconveniencias en términos de prácticas institucionales. Por eso, traemos aquí algunas definiciones que consideramos fundamentales distinguir, a los fines de clarificar el mapa conceptual de disciplinas y herramientas asociadas desde diversas aristas a la inteligencia criminal.

14. Por ejemplo, así lo establece el art. 8 de la Ley 27148 (Ley Orgánica del Ministerio Público Fiscal de la Nación).

La investigación criminal. Es posible identificar diferencias sustanciales entre la inteligencia criminal y la investigación penal[15]. La primera es que la inteligencia criminal permite tomar decisiones en el plano de la seguridad pública, la política criminal y la persecución penal. Es decir, la inteligencia es una herramienta para la investigación en tanto le permite producir conocimiento de calidad. Su vinculación no es de exclusividad ni de homogeneidad, sino de asistencia para la producción de información, sea en términos de evidencia o de orientación de líneas investigativas, según la decisión que con ella se desee tomar y los usos que se estimen pertinentes darle. Asimismo, otra distinción es que la investigación penal –preliminar y/o formalizada– se despliega para el esclarecimiento de un hecho del pasado, la individualización de sus autores/as, la obtención de las pruebas y el juzgamiento de las personas responsables (Ugarte, 2015, p. 46). La inteligencia criminal no se limita a ello como hemos visto. Así, se ha dicho que la inteligencia criminal no es sinónimo de investigación criminal (Ugarte, 2014: 46) y no deberían ser confundidas porque son actividades con objetivos distintos, con regulaciones, prohibiciones y habilitaciones disímiles.

Técnicas de investigación criminal. Las técnicas de investigación criminal se encuentran reguladas por los códigos procesales penales y las leyes penales especiales y buscan la obtención de datos e informaciones vinculadas a los intereses de un caso en concreto. Estas técnicas pueden ser de lo más variadas (seguimientos, rastreos y escuchas telefónicas, averiguaciones financieras, declaraciones, entre muchas otras), y siempre orientadas de manera tal que contribuyan a comprobar una teoría dentro de un caso penal. Por su parte, la inteligencia criminal tiene entre sus dimensiones la etapa de obtención de datos y puede hacer uso de las mismas técnicas que la investigación criminal, lo que en su entorno se llaman técnicas de recolección de información. Cuando alguna de ellas implica la posible vulneración de derechos constitucionales –por invadir la privacidad o la intimidad de las personas– requerirá también de la autorización de la judicatura competente. No deberían confundirse las técnicas de carácter secreto o subrepticias con la propia actividad de inteligencia, ya que puede hacer uso de ellas, como, de otras técnicas propias de la investigación social no secretas. Es común dentro de la jerga judicial la utilización de la palabra inteligencia para las técnicas secretas, por lo que esto suele generar confusión en torno al concepto de inteligencia criminal tal como así lo exponemos, que es mucho más amplio que la mera recolección de información y la técnica aplicada para ello.

15. Cabe hacer referencia únicamente a las investigaciones penales preliminares y formalizadas en tanto están focalizadas en el conocimiento de la actividad delictiva y la identificación de personas para atribuirles responsabilidad penal. Lo que las diferencia es que las primeras no fueron presentadas ante la judicatura -ya que se encuentran destinadas a reunir los elementos suficientes para la formalización de cargos, si correspondiere- y las segundas sí fueron presentadas. Como hemos dicho las investigaciones genéricas presentan la particularidad de ser una nueva herramienta a disposición de los MP que se emparenta con los objetivos y herramientas de la inteligencia criminal, ya que están abocadas al conocimiento de problemas criminales y sus regularidades, por lo que aquí la distinción se torna difusa.

Análisis criminal. Es una herramienta analítica para conocer la criminalidad, que tiene como objetivos la producción de información para tomar decisiones en el ámbito de la seguridad y la política criminal. Es una práctica complementaria y necesaria para los organismos que tienen la responsabilidad de tomar decisiones para reducir los índices delictuales (Tudela, 2012, p. 15) y se refiere al estudio de individuos, grupos, conductas o incidentes que pueden constituir delito, con el fin de identificar patrones, infractores, víctimas, tendencias y la estructura de oportunidades para su comisión, incluyendo factores que inciden en los problemas de inseguridad (Tudela, 2015, p. 141). Dentro del ciclo de la inteligencia criminal, esta herramienta será utilizada en cada dimensión, según las acciones que deban concretarse. Es una herramienta para el análisis de información que de allí surja. Sin embargo, el análisis criminal no debe ser asemejado a la inteligencia criminal porque no posee las habilitaciones, prohibiciones, ni tampoco se encuentra limitado al tipo de organizaciones que pueden hacer uso de la inteligencia criminal. El análisis criminal como herramienta analítica puede ser utilizado también por observatorios del delito y las violencias de la administración municipal, provincial y nacional, además de privados y de otras agencias destinadas al estudio de la criminalidad y afines.

Contrainteligencia criminal

La contrainteligencia criminal aún no posee desarrollo teórico en Argentina. A modo de aproximación, en el ámbito de la inteligencia criminal, podemos decir que implicaría una actividad tendiente, por un lado, a evitar el despliegue de la inteligencia de grupos delictivos y, por el otro, a impedir que las decisiones que deriven de la inteligencia criminal, tanto en el plano de la seguridad como en el plano de la política criminal y la persecución penal se vean vulneradas por actores del campo de la criminalidad que desarrollen acciones con el fin de entorpecerlas.

Deberían existir dependencias dentro de las organizaciones, principalmente las fuerzas policiales de prevención y las policías de investigaciones, que pueden hacer uso de la inteligencia criminal y que se aboquen a esta actividad, cuando sea necesaria. Actualmente no se encuentra regulada, siendo únicamente pensada para el ámbito de la inteligencia nacional, enmarcada en la AFI, y ello deriva de la estructura tradicional de "comunidad de inteligencia" en la cual las funciones y roles se encuentran desdibujadas.

2.

Límites a la actividad de inteligencia criminal

Límites a la actividad de inteligencia criminal

La actividad de inteligencia criminal se vincula con un amplio espectro de decisiones y, por ende, de diversas acciones y operaciones que pueden ser desplegadas –a lo largo de las dimensiones que la conforman–, que deberán ajustarse, entre otras cuestiones, a la evaluación de los principios de necesidad y pertinencia, utilidad, proporcionalidad y legalidad, más aún en los casos en que puedan verse afectados los derechos de privacidad e intimidad.

El principio de necesidad –o pertinencia– se fundamenta en los objetivos que se desean cumplir a partir de la inteligencia criminal y el modo en que ella debe desarrollarse para alcanzarlos. Es decir, el despliegue de la actividad de inteligencia y el modo en que se desarrolle debe partir de una evaluación que integre el tipo de decisión que se debe tomar, la información disponible y faltante y las herramientas que deberán ser aplicadas para obtenerla en tal caso. Si de dicho análisis se arriba a la conclusión de que la inteligencia criminal no es necesaria y/o pertinente, no debería desplegarse.

El principio de utilidad obedece a la evaluación de las capacidades y maximizaciones que podría brindar la actividad de inteligencia en relación con las decisiones que deben tomarse y los recursos que deben destinarse a ella. Entonces, una vez establecida su necesidad y/o pertinencia cabe preguntarse acerca de la utilidad de su desarrollo, y, aunque ello pueda ser de difícil diagnóstico, permite ponderar experiencias anteriores, recursos disponibles, ventajas y desventajas en función de diversas prioridades institucionales. Si la actividad de inteligencia criminal es necesaria, pero no útil, es decir que no permitiría alcanzar un grado mayor de conocimiento sobre el asunto, no debería desplegarse.

El principio de proporcionalidad implica una evaluación entre los fines perseguidos y los efectos no deseados que pudieran producirse a partir del uso de las herramientas aplicadas y los recursos destinados al despliegue de la inteligencia criminal. En función de este principio se desprende otro de gran importancia: el principio precautorio, que expresa que cuando un riesgo no es cuantificable, es preferible no asumirlo ya que no es posible dimensionar las consecuencias negativas que podría acarrear. Si la actividad de inteligencia criminal es necesaria y útil, pero las técnicas de recolección de información que deberían aplicarse, por ejemplo, no presentan proporcionalidad entre las afectaciones posibles a derechos fundamentales y los beneficios a obtenerse, no debería realizarse.

Por último, una vez que se han superado los umbrales de necesidad, utilidad y proporcionalidad, tanto en la decisión de utilizar la inteligencia criminal como en el modo en que se desarrollará, resta evaluar la legalidad que debe rodear la actividad y cada dimensión de su ciclo. Es decir, que las acciones y finalidades de la inteligencia criminal se encuentren reguladas por ley. Obviamente, en caso de que tanto las finalidades y las acciones no puedan cumplimentar con los parámetros que nuclean su legalidad (constitucional, legal y/o reglamentaria), la actividad no debería realizarse.

De esta manera, la legalidad, más allá de ajustarse a los mandatos constitucionales y la normativa internacional en materia de derechos humanos, debería estar delimitada por la organización que la emprenda y sus reglas propias, el modo en que la información debe ser recolectada y el uso que se le deba dar a dicho conocimiento en contextos particulares, entre otras variables. Esto es, deben existir diversos niveles de regulación que van desde el plano constitucional y legal (Constitución Nacional, tratados internacionales, Ley de I nteligencia Nacional, códigos procesales penales, leyes penales especiales, leyes orgánicas, entre otras) hasta normativa interna de las organizaciones (resoluciones, protocolos, reglamentos, entre otros), que atiendan a las distintas necesidades de la actividad de inteligencia criminal.

Recordemos que las actividades de inteligencia podrán orientarse a la toma de decisiones desde un nivel mayor de generalidad, como el diseño de la planificación de la seguridad, hasta aportar información en relación a un caso penal específico. En cada situación se aplicarán las habilitaciones y prohibiciones generales establecidas en los diversos niveles regulatorios mencionados.

El principio de legalidad, así, debe ponderar cuáles son las reglas que se deben cumplir para que dicha actividad de inteligencia pueda ser desplegada y el conocimiento producido sea válido y posible de utilizar. Es decir, el principio de legalidad involucra la ponderación de niveles de prohibiciones, permisos y autorizaciones, cuyo incumplimiento torna ilegal la actividad. Existen en este contexto situaciones que van desde las prohibiciones absolutas[16] hasta las que requieren diversos niveles de autorización en función de los derechos en juego y las jerarquías necesarias para su protección (autorización judicial[17], la autorización de las máximas autoridades de la organización y/o autorización de la

16. Para ejemplificar las prohibiciones absolutas, hacemos referencia a las vinculadas a su finalidad y a la dimensión de obtención de información del ciclo de inteligencia. Sobre la finalidad de la actividad de inteligencia, la ley 25520 en su art. 4, inc. 2, establece -en la actualidad- como prohibición absoluta obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción. Respecto de la dimensión de obtención de información, podemos mencionar la prohibición absoluta de obtener datos a través de la tortura, tratos crueles e inhumanos y hostigamiento de personas conforme a nuestra constitución y tratados internacionales. Estos son ejemplos dentro de la infinidad de prohibiciones absolutas que rodean a la actividad de inteligencia criminal conforme a la normativa actualmente regulatoria.

17. Por ejemplo, aquellas acciones que con el objetivo de obtener información pudieran afectar la intimidad y/o privacidad de las personas dada la técnica de recolección de información que debe ser utilizada, como pueden ser las intervenciones telefónicas, la utilización de agentes encubiertos/as, entre otras. Estas regulaciones pueden surgir de los códigos procesales penales, como así de leyes penales especiales, entre otras.

persona superior inmediata[18]). De igual modo, las consecuencias del incumplimiento de estas cuestiones pueden desencadenar desde la comisión de un delito hasta una sanción disciplinaria o una violación al código de ética interno de cada organización.

Por lo tanto, las reglas estarán dadas por las prohibiciones que la ley de inteligencia criminal establezca[19], como por diversos conjuntos normativos que deberán tender al aumento del control, la reducción de la discrecionalidad y la autonomía de quienes deben desarrollar la inteligencia criminal.

Dentro de la política criminal y la persecución penal rigen las reglas judiciales y garantías del debido proceso, en tanto el conocimiento obtenido pretenda ser utilizado en calidad de evidencia. Es decir, cuando la inteligencia resulta ser de utilidad para el MP o las fiscalías, la información sólo podrá ser incorporada como prueba a una causa judicial si cumple con las aptitudes dispuestas por la Constitución Nacional y las leyes que regulan el procedimiento penal. Pese a las distintas observaciones que podrían realizarse, resulta ser un ámbito más regulado y limitado, más difuso a medida que nos alejamos de la investigación formalizada y nos aproximamos a las investigaciones genéricas.

En el ámbito de la política de seguridad, las limitaciones aparecen más difusas aun, a pesar de tener como norte la utilización de fuerza estatal como último recurso y de aplicación excepcional. Es decir, cuando la inteligencia criminal se vincula con el ámbito de la seguridad pública, las actividades se tornan más opacas y con menos regulaciones[20]. Esto aumenta las posibilidades de discrecionalidad que podrían derivar en abusos de autoridad y/o afectación de garantías individuales.

De allí surge la necesidad de pensar una pronta regulación y transparencia en dirección a la democratización de la actividad de inteligencia criminal teniendo en cuenta lo mencionado hasta aquí y lo que sigue a continuación. Se trata de un nuevo escenario que requiere de normas, conceptos y doctrinas que enmarquen la actividad para contener el poder policial o punitivo del Estado (Estévez, 2015, p.235).

18. Por ejemplo, aquellas acciones dentro de la dimensión de obtención de información que en principio no afectarían derechos fundamentales, aunque posean determinado nivel de riesgo potencial. Entre ellas, podemos mencionar la obtención de información a partir de entrevistas o la observación de un territorio determinado sin reglas subrepticias. También ingresan aquí cuestiones propias de las dimensiones de registro, sistematización y recuperación de la información, que podrían ser ordenadas por el personal jerárquico.

19. Actualmente no existe una ley de inteligencia criminal en particular, sino que las regulaciones vinculadas a las prohibiciones se encuentran en la Ley de Inteligencia Nacional 25520, el Decreto 1311/2015 y sus anexos, en las disposiciones internas de los ministerios de seguridad y fuerzas policiales, los códigos procesales penales, las leyes penales especiales, la Constitución Nacional y los tratados internacionales de derechos humanos. También es posible encontrar limitaciones vinculadas a la ley de datos personales, acceso a la información pública, entre otras.

20. Vale mencionar como ejemplo de esto el Protocolo de Ciberpatrullaje RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018 sobre la implementación de la política de ciberpatrullaje. En este sentido, se tomó conocimiento público de ello recién en abril del 2020, a raíz de la discusión sobre ciberpatrullaje -abierta en ese momento- para reformarlo y dar origen al protocolo nuevo mencionado al comienzo de este documento.

No podemos negar que nos encontramos ante la necesidad de un cambio de rol de la seguridad y la política criminal, las cuales deben asumir roles activos y estratégicos. Por lo tanto, pensar en una actividad de inteligencia criminal eficaz pero estrictamente regulada para evitar la afectación de derechos es un desafío complejo que exige ser abordado con absoluta celeridad.

3.

Ciclo de información para la actividad de inteligencia criminal

Ciclo de información para la actividad de inteligencia criminal

Hemos mencionado que la inteligencia criminal conlleva un ciclo de información propio que se encuentra conformado por dimensiones en las que se despliegan diversas acciones y se identifican distintas necesidades, dificultades, prohibiciones y habilitaciones hasta alcanzar el conocimiento deseado para la toma de decisiones.

Todas estas dimensiones del ciclo de la inteligencia deben ser analizadas pragmáticamente desde los principios de necesidad y/o pertinencia, utilidad, proporcionalidad y legalidad.

Para ello, es útil generar al interior de las instituciones las reglamentaciones necesarias para el ciclo de inteligencia criminal a los fines de resguardar su transparencia y accesibilidad, en los puntos en que ello sea posible. Es decir, adecuar la regulación interna organizacional a la normativa aplicable para que sea posible conocer qué tipo de tecnologías se utilizan en cada dimensión, bajo qué parámetros se realizan las búsquedas de datos, dónde quedan registrados, qué sucede con la información que se considera inútil o impertinente, qué condiciones de guarda y de seguridad poseen las informaciones producidas, qué tipo de profesionales trabajan en las organizaciones abocadas a la inteligencia, con qué presupuestos y recursos se cuenta, entre otras cuestiones. Ahora bien, las dimensiones que pasamos a describir a continuación conforman una propuesta metodológica pensada concretamente para trabajar en el ciclo de información de la inteligencia criminal. Debemos advertir que, aunque se hable de ciclo o de proceso, en la producción de inteligencia las dimensiones no se concatenan cronológicamente en sentido lineal hasta llegar al producto final, sino que pueden existir avances y retrocesos en relación a la evolución de la producción de información. En este sentido, se ha advertido que la denominación de ciclo puede llevar a error si se piensa que sólo tiene un inicio y un final, y así vuelve a repetirse, pero se ha consensuado atribuir esa denominación porque facilita enormemente su comprensión y sus efectos didácticos (Jiménez Villalonga, 2020, p.2).

Por último, y antes de adentrarnos en las dimensiones, resaltamos que es imprescindible que cada ciclo de inteligencia criminal se desate en relación a un proceso de planificación previo que determine las motivaciones, necesidades, sospechas y/o hipótesis que lo hacen pertinente en relación a la criminalidad y las violencias en el marco de la política de seguridad, la política criminal o la persecución penal.

La fundamentación de cada ciclo debe ser detallada y tener su registro con el objetivo de garantizar un control interno y externo y así disminuir los niveles de discrecionalidad y autoritarismo en que podrían incurrir las diversas organizaciones. Esto es lo primero que debe hacerse antes de avanzar sobre cada dimensión del ciclo de la inteligencia.

Dimensiones del ciclo

El ciclo de la inteligencia criminal podría estar conformado por las siguientes dimensiones, orientadas a ordenar los puntos centrales para producir conocimiento para la toma de decisiones en los planos que hemos indicado en términos de seguridad, política criminal y persecución penal.

Dimensión 1. Obtención

Es la primera dimensión del ciclo y consiste en la acción orientada a la adquisición y reunión de información y/o datos en bruto (Navarro Bonilla, 2004). Inicia el ciclo, ya que es la dimensión en la cual se recolectan todos los datos e informaciones que van a ser utilizados en su posterior desarrollo hasta llegar a la confección del reporte o elaboración del conocimiento. Por lo tanto, aquí se definen los tipos de datos e informaciones pertinentes, las fuentes de información a ser consultadas, las técnicas de recolección que serán necesarias y las personas que intervendrán en esta instancia en calidad de recolectoras.
En función de estos cuatro ejes giran las precisiones de esta dimensión, las cuales se encuentran plenamente ligadas a la problemática a analizar en el despliegue de la actividad de inteligencia criminal. Es una dimensión que requiere de conocimientos especializados y profesionalizados, ya que constituye la columna vertebral de todo el ciclo.

Es importante destacar que la mayor parte de las regulaciones y límites de la actividad de inteligencia criminal versarán sobre esta primera dimensión, ya que las acciones que la componen se dirigen a grupos, personas y/o situaciones que constituyen el objeto de producción de información. En este sentido, y con el objetivo de maximizar el resguardo por las garantías constitucionales y ajustar estas acciones al marco de los principios de necesidad y/o pertinencia, utilidad, proporcionalidad y legalidad, las acciones de esta fase deberán circunscribirse bajo ciertas normas.

Uno de los atributos de esta dimensión debería ser el cumplimiento del principio de minimización[21]. Este principio consiste en orientar la recolección hacia la información que es pertinente y en el descarte de toda la información trivial por parte de las personas que cumplan la función de recolección. De este

21. Aunque es un principio que debe recorrer cada una de las dimensiones dada su relevancia para el respeto de los derechos y garantías constitucionales. Es un principio que necesariamente se vincula con las limitaciones de la actividad de inteligencia criminal que hemos mencionado más arriba.

modo, no sólo se busca evitar el ingreso al registro de información no relevante, sino impedir que información que pudiera afectar a terceros/as pase a formar parte de una base de datos de información criminal.

A continuación, se mencionan las características de los diferentes tipos de fuentes de información según su origen y niveles de accesibilidad a las que puede recurrirse. Finalmente, se desarrollan algunas de las diferentes técnicas de recolección de información que pueden ser utilizadas en el marco del desarrollo de la inteligencia criminal.

Fuentes de información

Las categorías y características aquí desarrolladas en términos de fuentes son meramente analíticas para poder brindar un sentido y orden explicativo. Las diversas fuentes de información pueden presentar condiciones entrecruzadas mucho más amplias que las que aquí mencionamos a modo de ejemplo.

→ Según sea propia o ajena su producción

La distinción más general que hacemos se basa en la información producida por las propias personas encargadas del ciclo de la inteligencia criminal y la que obtienen de fuentes externas, o es producida por otras personas, organizaciones, etc. Así, teniendo en cuenta la variedad y volumen de las fuentes podemos diferenciar sintéticamente dos tipos que se vinculan con las demás categorías que desarrollaremos:

Información primaria: se refiere a la que se consigue mediante la aplicación de una o varias técnicas de obtención de datos producida a los fines de la propia investigación (Cea D'Ancona, 1996, p. 220). Es decir, la que se produce por las propias personas, sea a través de medios no secretos y secretos (personas encubiertas en calidad de agentes, intervenciones telefónicas, entrevistas, observación, etc.).

Información secundaria: engloba tanto los datos "brutos", elaborados por terceros/as u otros organismos para sus propios propósitos, como los proporcionados y analizados en distintas publicaciones. Las fuentes secundarias se consideran extensión y punto de partida habitual de la indagación primaria (D'Ancona, 1996, p. 222). Pueden encontrarse aquí estadísticas producidas por oficinas de la misma organización, bases de datos ajenas ya elaboradas, publicaciones oficiales, académicas, entre otras.

Ambos tipos de fuentes no constituyen modalidades contrapuestas sino complementarias y, como regla general, se vinculan y cruzan con el resto de las categorías que describiremos.

→ Según su origen o medio en el que se encuentre

Los tipos de fuentes varían de acuerdo a cómo la información se encuentra presentada, lo cual, a su vez, condicionará los medios y herramientas para su accesibilidad. Si bien en la literatura normalmente se define a los tipos de fuentes de información como tipos de inteligencia propiamente dichas (por ejemplo, inteligencia de fuentes digitales) aquí las desarrollaremos como fuentes de obtención de datos e información a ser utilizadas por la inteligencia criminal y no como un tipo de inteligencia en particular. No haremos un detalle extenso de todas las fuentes de información, sino de las principales que sirven como guía.

Humanas (conocidas como HUMINT - *human intelligence*): considerada como una de las primeras fuentes de la inteligencia. La fuente de información es la humana –personas físicas– sea a través de sus palabras y/o sus acciones. Así, es entendida como la obtención de datos de persona a persona, permitiendo captar información usando tanto medios tecnológicos como no y pudiendo utilizar métodos abiertos como clasificados, de acuerdo a los requerimientos del ciclo (Korkisch, 2010, p.37). La persona encargada de su recolección debe tener un entrenamiento particular según el tipo de técnicas de recolección de datos que se precise emplear.

Medios tecnológicos (TECHINT - *technical intelligence*): consiste en la recopilación de datos e información en medios tecnológicos. Estas fuentes están vinculadas a equipos y/o sistemas de almacenamiento de información de diversa índole y magnitud, que van desde bases de datos o equipos audiovisuales, hasta las distintas fuentes de acceso digital. Dado que el espectro de estas fuentes es muy amplio, existen una serie de técnicas distintas para extraer información. No todas las plataformas en las que se presenta la información de tipo tecnológica son accesibles e inteligibles directamente por una persona analista y pueden requerir la utilización de métodos artificiales. Esto normalmente sucede con la información que se encuentra en grandes volúmenes de datos (*big data*) que necesitan ser filtrados y procesados o que se presenta con algún tipo de codificación (Omand, Bartlett y Miller, 2012, p. 810). Por ejemplo, es conocida la *machine learning* como una técnica que utiliza algoritmos para reconocer distintos patrones en la información pudiendo extraer el significado de ella de una forma que no podría hacerlo un analista humano. En definitiva, según el medio tecnológico del cual se quiera extraer información, existirán diversas herramientas de obtención y capacidades que deberán ser aplicadas.

Señales (SIGINT - *signal intelligence*): la fuente de información de señales consiste en recopilar datos e información a partir de diversos sistemas de comunicación. Es una categoría que abarca a las fuentes compuestas por sistemas electrónicos y captación de señales e instrumentación, cualquiera sea su forma de transmisión (Department of the

Army USA, 2006, p. 217). Como normalmente mucha de esta información se encuentra codificada, las personas expertas en la materia deben desarrollar y emplear herramientas y sistemas de última generación que faciliten la obtención de estos datos en el cambiante entorno actual de las comunicaciones y la información (NSA, 2021).

Digitales Abiertas (OSINT - *open source intelligence):* son fuentes digitales de acceso público (Steele, 1997, p.329). Se han convertido en uno de los tipos más relevantes de fuentes de información, ya que los avances en el campo digital han aumentado significativamente en torno a su cantidad, importancia y accesibilidad (Public Law, 2006, p. 109-163). Entre este tipo de fuentes podemos encontrar:

- **Medios de comunicación:** que incluyen diarios, revistas, radio, televisión y todo tipo de portal web digital.

- **Información pública oficial:** dentro de ella está la información derivada de informes gubernamentales, datos oficiales –como datos sobre presupuestos y demografía–, audiencias y debates legislativos, conferencias de prensa, discursos, directorios, organigramas, entre otros.

- **Literatura gris:** consiste en todo el material que se encuentra normalmente disponible bajo acceso controlado para un público específico. Por ejemplo, informes de investigación, técnicos, económicos, *papers*, estudios, disertaciones, entre tantas otras publicaciones (DNI, 2013, p. 47).

- **Redes sociales y medios digitales:** conocida como SOCMINT (inteligencia en redes sociales) por sus siglas en inglés (Estévez, 2014, p. 70). Este tipo de fuente en particular se basa en perfiles, blogs, aplicaciones y todo tipo de sitio de interacción social digital que se encuentre abierto al acceso público.

Uno de los principales dilemas que giran en torno a la utilización de las fuentes SOCMINT es establecer una frontera clara entre lo que es el espacio digital público y el espacio digital privado, lo cual deberá ser debidamente diferenciado para garantizar regulaciones con respecto al uso de esa información (Estévez, 2014, p.70).

Aquí los debates giran en torno a la privacidad de los perfiles públicos en las redes sociales ya que, si bien su acceso es abierto al público en general, las personas presuponen una expectativa razonable de privacidad al momento de publicar sus contenidos. En este sentido, Edwards y Urquhart (2015, p. 15) advierten tres objeciones a la presunción obvia de que las fuentes SOCMINT carecen de privacidad o que son abiertamente públicas. La primera es la recolección de información a partir del círculo de contactos que cada persona posee en su red social. Es decir, resulta muy complejo lograr escudar a todos los contactos que poseen

las personas sobre las cuales se busca recolectar la información. En segundo lugar, no debería hacerse uso del contenido de terceros/as que aparece en los perfiles públicos sin que los primeros hayan autorizado su publicación. Muchas veces, inclusive, la información de terceros/as que aparece en un perfil pudo no haber sido publicada por el titular de esa cuenta sino asociada por una etiqueta o compartida desde otra cuenta a ese perfil. En tercer lugar, la configuración de la privacidad en cada sitio suele ser demasiado extensa, estar escrita con un vocabulario complejo o ser cambiante, lo que hace difícil a las personas configurarla de un modo tal que impida cualquier acceso que no desee. Esto tiene como consecuencia que muchas cuentas sean públicas aun cuando su titular consideró haber establecido su privacidad. Por lo tanto, se puede observar que no todas las fuentes digitales son abiertas y/o públicas. Asimismo, el hecho de que algunas pudieran estar configuradas como tales, no implica la posibilidad de un acceso y uso irrestricto de la información, sobre todo teniendo en cuenta que la mayoría de este contenido es información personal o permite inferir datos personales de diversa índole.

Existe actualmente un vacío legislativo en nuestro país en relación a las tecnologías y formas de incursionar en determinadas fuentes de información como las digitales, lo que requiere de un proceso de discusión por el tipo de afectaciones a la privacidad e intimidad de las personas que pueden desencadenar. Más aún teniendo en cuenta que, en gran medida, la obtención de datos no puede realizarse de manera humana, sino que deben ser utilizadas tecnologías de automatización artificiales. De esta forma, es necesario empezar a discutir sobre estas técnicas y fuentes para establecer las regulaciones pertinentes en cada caso, como se ha regulado la fuente humana de información y sus modos legales de obtención.

→ Según su nivel de accesibilidad

Los diversos orígenes de la información –o medios de los cuales se obtienen– pueden tener distintas habilitaciones y/o posibilidades de acceso:

Abierta: la información de fuentes abiertas es aquella que se encuentra disponible públicamente para todas las personas que quisieran acceder a ella. No se requiere de ningún tipo de autorización para obtenerla. Es información no clasificada que puede tener su origen en las diversas fuentes que hemos señalado en forma precedente. El gran volumen de información que puede llegar a involucrar, dada esta condición de accesibilidad, hace necesario que haya analistas con suficiente formación para su obtención y recorte, así como de tecnologías particulares de rastreo.

Restringida: la información en este tipo de fuente es aquella que puede ser recolectada con acceso y disponibilidad limitada al público general. El término restringido hace referencia a que en general se precisa de claves habilitadas o accesos particulares autorizados sin los cuales no es posible obtener la información.

Clasificada: es información que no se encuentra disponible sin habilitaciones excepcionales –desclasificaciones– o que requieren de la utilización de técnicas de recolección de información secretas, humanas y tecnológicas, para ser obtenidas. Este tipo de información requerirá para ser obtenida diversos tipos de autorizaciones judiciales e internas de la organización dado el riesgo que existe de vulnerar la privacidad y la intimidad de las personas involucradas. Asimismo, existen mayores restricciones al momento de la difusión de los reportes que la incorporan, ya que contará con datos que no siempre podrán ser publicados sin autorización (United Nations Office on Drugs and Crime, 2011).

Técnicas de recolección de información

Históricamente, se ha asociado a la inteligencia criminal con técnicas de recolección de información secretas que, si bien son características de la actividad, no son las únicas. Ya hemos hecho referencia a que la inteligencia criminal puede recurrir a diversas fuentes de información y a distintas técnicas para la obtención de datos para analizar. Todas ellas requieren de la evaluación de necesidad y/o pertinencia, utilidad, proporcionalidad y legalidad, más aún aquellas secretas –en las cuales las personas no saben que están siendo escuchadas, leídas, observadas– y pueden verse afectados derechos constitucionales como la privacidad y la intimidad.

En este sentido, los estados democráticos no se pueden privar de tener un sistema de inteligencia criminal capaz de garantizar la seguridad de la ciudadanía y la toma de decisiones eficientes y eficaces, por lo que en determinadas ocasiones las esferas de la privacidad y la intimidad ceden ante las necesidades estatales. Dado el peligro que ello representa, las acciones que pueden afectar estos derechos fundamentales deben ser restringidas, regladas y sumamente controladas.

En estos casos, y con el objetivo de garantizar la excepcionalidad de su utilización, deberá requerirse autorización judicial. Extrapolando las similitudes, el Anteproyecto de Ley de Inteligencia Nacional señala que las técnicas de captación de comunicaciones, flujos de datos y cualquier otro tipo de actividades que impliquen la intromisión en la privacidad de las personas, deberán ser autorizadas judicialmente, especificando el objeto de la solicitud y el plazo necesario para explotar la fuente de información (proyecto de ley elaborado por Consejo Consultivo de la AFI, 2021, art. 9, p.10).

Enumeramos algunas de las técnicas de recolección de información que pueden utilizarse durante la actividad de inteligencia, algunas de ellas son reguladas como técnicas de investigación criminal en las leyes correspondientes y otras tienen su origen en las técnicas de la investigación social.

Observación: por definición, es el modo de establecer algún tipo de contacto empírico con los objetos, sujetos, situaciones de interés con el fin de su descripción, explicación, comprensión, etc. Puede ser humana o bien tecnológica. Existen diferentes formas de definirla según sea directa o indirecta, esto es, si se recolecta información directamente o

mediada por observaciones realizadas previamente. Además, otras maneras incluyen a la observación estructurada o no estructurada, según el grado de sistematicidad y de delimitación previa de qué/quién, cómo y cuándo (Marradi, Archenti y Piovani, 2007, p. 193).

Seguimiento: dentro de las técnicas de observación en la inteligencia pueden mencionarse los seguimientos a pie, a través de vehículos y otras tecnologías, de personas y/o grupos de personas objetivos.

Agente secreto/ acciones encubiertas: infiltraciones secretas, humanas y tecnológicas, en un contexto determinado con el fin de reunir información de diversa índole sobre el asunto a atender. La característica central es que se desconoce la identidad real de la persona, la presencia de la misma o de la tecnología aplicada.

Interceptación de comunicaciones/ conversaciones: comprende la captación de comunicaciones privadas de voz, cara a cara, correos, paquetes de datos, sistemas de información privados y/o documentos físicos en diversos formatos.

Captación de imágenes: toma de imágenes fotográficas y/o imágenes de video en espacios públicos o privados de personas, situaciones, lugares, entre otras.

Entrevista: conversaciones que se desarrollan entre la persona recolectora de información y la/s persona/s objetivo/s. La particularidad es que la entrevista se encuentra direccionada con preguntas concretas u orientadas a la obtención de determinados datos y no suele ser una conversación abierta y exploratoria como puede desplegarse en el marco de las acciones encubiertas humanas. Cada persona realiza una entrevista diferente en función de su cultura, sensibilidad y conocimiento sobre el tema y, sobre todo, según el contexto espacio-temporal en el que se desarrolla la misma (Alonso, 1998, p.79). Sin embargo, es fundamental el entrenamiento de las personas a cargo en herramientas cognitivas, emocionales y de comunicación.

Sondeo: es la aplicación de un procedimiento estandarizado para recolectar información –oral o escrita– de una muestra de personas acerca de los aspectos estructurales, ya sean ciertas características sociodemográficas u opiniones acerca de temas específicos. La información se recoge de forma estructurada y el estímulo es el mismo para todas las personas (Cea D´Ancona, 1996, p. 240).

Solicitud de información a diversos organismos: esto implica la solicitud de diversa información –sobre personas, situaciones, territorios, etc.– sobre la cual habrá que atender los niveles de accesibilidad y secreto que posean tanto para su requerimiento y permisos, como para su divulgación en los reportes.

Búsqueda personalizada: es aquella actividad orientada a la obtención de datos e información en forma personal y directa de forma exploratoria a partir de diversas fuentes de información. Por ejemplo, búsquedas en fuentes digitales, libros, bases de datos, noticias, entre otras.

Estas son solo algunas técnicas de recolección de información que hemos seleccionado para ilustrar que la actividad de inteligencia puede utilizar técnicas secretas y no secretas, en función del tipo de información que se desea obtener, las condiciones en que las que se encuentra y el ámbito en que se desarrolla. Reiteramos que se deben evaluar siempre los principios mencionados antes de desplegar cualquiera de ellas, aunque sin duda los criterios de protección se robustecen en la medida en que alguna de las técnicas de recolección de información pueda afectar, en mayor o menor medida, la intimidad y la privacidad de las personas.

Es fácil observar que la dimensión de obtención tendrá que ser desarrollada por equipos interdisciplinarios que manejen conocimientos particulares, tanto de fuentes de información como de recolección de datos, dadas sus condiciones especiales y diferencias. Incluso, el asunto a abordar será también clave para la selección del personal a cargo del ciclo en su totalidad.

Dimensión 2. Registro

El registro consiste en la clasificación, el guardado y el almacenamiento de los datos y la información obtenida en la etapa anterior de un modo organizado, en función de diversas categorías que resulten útiles a fines de los objetivos propuestos.

En esta dimensión se toman decisiones vinculadas al modo de registrar y acopiar la información, en función de, por ejemplo, diversas variables como la fuente de origen, la accesibilidad, el tipo de producción –propia o ajena–, por credibilidad, por tema que aborda, entre otras. Existen un sinfin de posibilidades, que se vincula en forma directa con el asunto que se aborde desde el ciclo de inteligencia criminal.

Durante esta etapa también se puede evaluar la eficacia de las técnicas y métodos de recolección de información en relación con cada búsqueda. Esto significa que durante el registro se puede medir el porcentaje de información que ha sido finalmente relevante a los fines del ciclo y qué porcentaje de información resultó irrelevante. De este modo, se define la precisión y eficiencia de las técnicas de recolección.

Por otro lado, más allá de la clasificación primaria de los datos e informaciones, esta dimensión tiene el objetivo de establecer criterios ordenatorios que permitan el control y el seguimiento de la información. Esto es, el registro exhaustivo de qué ingresa al ciclo y qué es eliminado –con sus autorizaciones y fundamentaciones pertinentes–, el modo en que ingresa –cómo y quién lo recopiló–, el lugar de almacenamiento, el tiempo por el cual será guardada, las

condiciones de seguridad, las pautas para su destrucción y las autorizaciones judiciales y/o internas de la organización que se hayan tenido que solicitar para su obtención, entre otros ejes.

Es importante definir los atributos que conformarán al registro ya que a partir de ello no sólo se hará una mejor sistematización de la información, sino que se le otorgará un marco de regulación y previsibilidad a la manera en que se acopia la información recolectada. Estos atributos definidos previamente deberán cumplirse en relación con los medios donde la información finalmente sea registrada.

Cobra nuevamente interés aquí el principio de minimización, mencionado anteriormente, para toda aquella información que fue recolectada en la fase anterior pero que se descubre que no será útil a los fines del ciclo. En este sentido, esta información deberá ser "minimizada" para impedir que sea registrada cuando no sirva a los propósitos del ciclo iniciado.

Esta dimensión tiene estrechas implicancias con la protección de datos personales, el acceso a la información pública y las limitaciones propias de la inteligencia sobre qué tipo de información puede recopilar sobre las personas y cuáles se encuentran prohibidas. Por eso, entendemos que debe existir una armoniosa convivencia entre las normas que regulan los mencionados aspectos y todo el ciclo de inteligencia criminal, las cuales deben ser salvaguardadas aquí en particular.

Dimensión 3. Sistematización

La sistematización de la información consiste en el ordenamiento de los datos y la información previamente registrada para que la persona que oficie de analista pueda acceder a ella de una forma sencilla y eficiente (FAO, 2004). Se diferencia del registro porque no apunta a su control y seguimiento, sino al desglose de los datos y las informaciones conforme a categorías analíticas de utilidad de cara a hacerlos observables para quien los analice.

Esto implica, entre otras cosas, la construcción de bases de datos, la definición de variables e indicadores para su análisis, la separación y ordenamiento en función de ejes analíticos y la selección de diversas tecnologías para su entrecruzamiento y visualización.

Sobre algunos de estos puntos se ha dicho que, por ejemplo, la cuantificación de los distintos aspectos de la información mediante indicadores sólidos resultará de extrema relevancia. Estos deben ser adecuados a los fenómenos –o asuntos– que se quieren analizar, y aportarán la información necesaria para gestionar la información para su análisis. Por su parte, los sistemas de información deben alcanzar armonía y coordinación para facilitar una visión sistémica de los fenómenos (Sistema Regional de Indicadores Estandarizados de Convivencia y Seguridad Ciudadana, 2012, p. 24).

En esta dimensión, la información se ordena bajo determinados criterios a través de una variedad de métodos como son la depuración, traducción, valoración, reducción, y correlación de datos, llevados adelante por analistas con formación apropiada, quienes sistematizarán la información en base a un criterio previo acorde a lo que se está trabajando y al tipo de información obtenida previamente (Centro de Inteligencia Prospectiva, 2010, p.7).

De esta etapa podrán encargarse tanto quienes hayan formado parte de etapas anteriores como no, de acuerdo a la decisión que se tome dentro de cada ciclo. Sin embargo, se aconseja que para sistematizar una experiencia, es preferible escoger a quienes han formado parte de ella y no a quienes se hayan mantenido ajenos. (Jara, 1994, p. 94).

Lo imprescindible de esta instancia es que la información quede ordenada en función de maximizar su utilidad, sin que se pierdan datos o informaciones relevantes y de manera tal que queden asegurados para la instancia de análisis, agotando al máximo posible su depuración. Entre otras cosas, esta dimensión contribuye a evitar:

- la repetición de datos e informaciones;
- el ingreso de información impertinente al análisis;
- el ingreso de información de baja calidad;
- el faltante de información indispensable; y,
- la desorganización de los datos y la información.

Dimensión 4. Recuperación

En esta dimensión se resuelven cuestiones de accesibilidad de las bases de datos e información recopilada, tanto para las personas agentes de inteligencia criminal como hacía afuera del organismo y dependencias internas. Existirá información diferenciada según su clasificación y corresponderá establecer niveles de acceso para determinar quiénes podrán hacer uso de ella y en qué medida.

Dimensión 5. Análisis

Se entiende al análisis como el uso de la información sistematizada para interpretarla y describirla con el fin de responder a las preguntas ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué?, y ¿para qué?; y la construcción de hipótesis finales que sirvan a la toma de decisiones. Es decir, consiste en separar la información, en sus diferentes componentes, comprobar su veracidad, utilidad y exactitud para evaluarlos y examinarlos.

En esta dimensión también se realiza el último filtrado y descarte de la información que no es pertinente con el fin de preservar los datos que contribuyan a formular el problema e indicar la información restante, si es que fuera necesaria su obtención. De este modo, como resultado del análisis debería surgir:

- ¿Cuál es el problema? Alcance, dimensiones, regularidades, manifestaciones, entre otras. Esto es, intentar responder a las preguntas señaladas previamente para la construcción de la hipótesis.

- ¿Qué información se registró hasta ahora o deberían obtenerse más adelante para completar las respuestas pendientes?

- Favorecer la identificación del mapa de actores que podrían involucrarse en el asunto.

- Hipótesis que orienten la toma de decisiones.

Asimismo, algunos aspectos a tener en cuenta dentro de esta dimensión refieren a que los criterios de análisis idealmente deberían estar libres de sesgos, prejuicios y de influencias. Además, el análisis debería ser realizado de manera especializada por personas analistas expertas en el asunto y con la suficiente independencia en el despliegue, para un resultado desprovisto de cualquier omisión de información relevante para la toma de decisiones, como así, de interpretaciones forzadas que se no desprendan adecuadamente de la información.

Sobre el cuerpo de analistas, se considera pertinente trabajar con interdisciplinariedad y especializaciones. En este sentido, Evans (2014, p.24) afirma que un modelo de inteligencia eficiente debería integrar a la mayor cantidad de actores relevantes en la producción de información y conocimiento sobre la seguridad pública para poder abordar integralmente los fenómenos delictivos de interés para dicho modelo. Sugiere, además, la necesidad de que las personas que se desempeñan como analistas se encuentren permanentemente en formación y perfeccionamiento con el objetivo de desarrollar una carrera a largo plazo y aumentar su *expertise* en el área.

Con respecto a la creación de equipos interdisciplinarios, David Omand (2013, p. 816) remarca la necesidad de complementar mejor las disciplinas humanísticas con las computacionales y estadísticas a la hora de comprender de forma precisa aquella información que sea recolectada. A su vez, sugiere que las disciplinas del campo social, como la psicología, la ciencia política o la sociología, suministren el análisis del comportamiento social y subjetivo a la información recolectada, por ejemplo, a través de las técnicas de *big data* en la que se recopila un gran volumen de información. Por último, remarca que la solidez metodológica de la actividad de inteligencia depende de una nueva interdisciplina académica que fusione los enfoques humanos, tecnológicos y computacionales.

De esta manera, la conformación de equipos interdisciplinarios que trabajen integradamente, aplicando distintas disciplinas científicas y técnicas, llevará a un análisis más completo y preciso que tendrá como corolario la formulación de decisiones y de políticas mejor dirigidas.

Dimensión 6. Reporte

Esta dimensión responde a la elaboración del reporte, el cual presentará condiciones propias de acuerdo al objeto de estudio y a la persona destinataria para la cual se realiza. Puede tener distintos formatos, digitales, verbales o en papel, según las urgencias y particularidades de la actividad de inteligencia criminal.

Si bien, cada reporte tendrá su estilo, mencionaremos a continuación algunas características generales que deben prevalecer (Jordan, 2016, p.18):

- Ser sintético y conciso, ya que busca exponer de manera focalizada lo que pretende comunicar, informar y/o alertar.
- Destacar lo relevante y hacia dónde fue dirigido el análisis de los datos y la información.
- Ser preciso, sin presentar lenguaje que se preste a confusiones ya que la ambigüedad conlleva que el reporte pierda credibilidad.
- Permitir evaluar el asunto y tomar decisiones, evitando que se fuercen conclusiones no fundamentadas de forma íntegra.

En esta dimensión se verán plasmadas todas las decisiones vinculadas a las dimensiones anteriores. El reporte debe contener la información relevante, dejando por fuera aquella que no contribuya a la toma de decisiones, y debe ser autosuficiente. Es decir, abarcar todos los puntos pertinentes sin necesidad de abastecerse de otro tipo de documentación y/o información.

Dimensión 7. Difusión

Esta dimensión consiste en la entrega del producto a las personas decisoras y destinatarias del reporte garantizando su seguridad. Uno de los desafíos de la difusión es que logre llegar a estas personas y que utilicen el conocimiento producido para valorarlo y tomar decisiones. También puede ser distribuido a otro cuerpo de analistas y/o diversas personas que se considere oportuno para la reorientación, profundización y retroalimentación del producto.

Asimismo, los niveles de accesibilidad del reporte y de su contenido son definidos en esta instancia. Aquí cabe mencionar que, en nuestro país, la Ley Nacional de Inteligencia establece tres categorías de clasificación de la información en poder de los órganos que componen el Sistema de Inteligencia Nacional: secreta, confidencial y pública, según el grado de compromiso que su divulgación implique para la defensa o seguridad nacional. Esta clasificación se encuentra establecida actualmente en su art. 16 bis y fue introducida a través de la ley 27126 de 2015, con la intención de reducir, en alguna medida, el secreto en el que tradicionalmente se vieron envueltas las actividades de inteligencia en nuestro país.

Con este mismo propósito, el Anteproyecto de Ley de Inteligencia desarrollado por el Consejo Consultivo de la AFI propone invertir el principio general y establece que la información debe ser pública salvo que excepcionalmente deba ser clasificada en los términos que establece el proyecto. Para estos casos, regula tres tipos de clasificaciones según el grado de resguardo que deba garantizarse. Esto propone una mirada nueva basada en la transparencia de las actividades del Estado, como regla.

Así, establece, por un lado que las actividades, el personal, los bancos de datos y la documentación producida por los organismos de inteligencia deberían ser públicas y sólo en los casos donde la producción de informes contenga información que no pueda ser divulgada, se mantendría el carácter confidencial, secreto y especialmente secreto de acuerdo a la categoría que corresponda (2020, arts. 11 y 12, p. 11 y 12). Por otro lado, propone las clasificaciones "confidencial" y "secreta" según el nivel de compromiso que pueda generar, y "especialmente secreta" cuando deba ser únicamente conocida por las personas que deben tomar decisiones en consecuencia.

Esto podría ser igualmente aplicado al ámbito de la inteligencia criminal, en el ámbito de la seguridad pública, la política criminal y la persecución penal. Al respecto de la inteligencia producida en el contexto de una causa penal deberán establecerse otro tipo de condiciones y resguardos, dados los objetivos que persigue y los derechos en perspectiva vinculados al ejercicio de defensa. De esta manera, pueden utilizarse las clasificaciones propuestas en función del compromiso que signifiquen para el cumplimiento de ciertas actividades de inteligencia criminal.

La razón principal de revertir el criterio y establecer la publicidad es evitar que el secreto siga siendo la regla en la actuación de los organismos de inteligencia criminal y posibilitar el control interno y externo. Es decir, que el modo de accionar de la inteligencia criminal sea accesible públicamente permite establecer una *accountability* de estos organismos no sólo desde el Estado, sino también desde la propia ciudadanía, a la cual se le ha vedado históricamente cualquier tipo de conocimiento en relación con la producción de inteligencia criminal.

Consideraciones sobre el ciclo de inteligencia criminal

El ciclo de la inteligencia criminal se puede conformar por estas dimensiones, las cuales deben ser reguladas mediante leyes, protocolos y reglamentaciones institucionales que den cuenta de su funcionamiento conforme a los puntos que fuimos desarrollando y otros tantos que aquí no se han tratado y restan profundizar.

Lo sustancial en el ciclo de inteligencia es establecer los límites y controles necesarios de cada dimensión con el fin de resguardar los derechos constitucionales que pueden verse afectados, como de, generar las condiciones propicias para tomar mejores decisiones en el ámbito público abocado al impacto sobre la criminalidad.

A la par será necesario regular por ley cuestiones vinculadas a las fuentes de información disponibles, las nuevas tecnologías y las técnicas de recolección de información sin las cuales no es posible hacerse de las informaciones y datos pertinentes para la inteligencia en la actualidad.

4.

Una ventana epistémica: las discusiones sobre inteligencia en fuentes abiertas y redes sociales

Una ventana epistémica: las discusiones sobre inteligencia en fuentes abiertas y redes sociales

Como suele ocurrir con los fenómenos novedosos, la problematización de esta cuestión se viene dando a través de un uso difuso de las categorías de análisis y reflexión (como en el caso del omnipresente prefijo "ciber-"), y también extrapolando, sin demasiado rigor, aspectos de lógicas "*offline*", ya conocidas, a funcionamientos "*online*".

En este campo complejo se insertan los debates acerca de la actividad de inteligencia criminal utilizando fuentes abiertas y redes sociales. Esto se conceptualiza como parte del trabajo de inteligencia con intersección entre las fuentes tecnológicas (TECHINT), las fuentes digitales abiertas (OSINT) y las redes sociales y medios digitales (SOCMINT). Se trata de fuentes de información para la inteligencia criminal sobre las cuales se produjo más literatura en los últimos años a nivel internacional, por su novedad y por las técnicas que deben ser aplicadas para su exploración.

En la Argentina, la doctrina del secreto que envuelve las decisiones ligadas al funcionamiento de los organismos que realizan tareas de inteligencia se extendió también a este ámbito, por lo que la actividad de inteligencia criminal sobre fuentes abiertas se fue implementando *de facto*.

Así lo evidencia, por ejemplo, la decisión del gobierno argentino de prohibir la participación de 65 activistas en la Conferencia Ministerial de la Organización Mundial del Comercio, que se celebró en la Ciudad Autónoma de Buenos Aires (CABA) en diciembre de 2017, justificada a partir de supuestos "llamamientos a la violencia" que estas personas habrían realizado en redes sociales. También, los casos de personas investigadas y judicializadas por escribir *tuits* amenazantes contra funcionarios/as que en los últimos años instalaron la noción de *ciberpatrullaje* y fueron naturalizando, tanto en el Poder Ejecutivo como en el Judicial y luego en los medios masivos, la idea de que la policía puede realizar tareas de *prevención* del delito en Internet sin que medie discusión pública sobre las características, límites y necesidad de regulaciones específicas de estas tareas (Asociación por los Derechos Civiles, 2018).

Podemos brindar otro ejemplo claro de la firme vigencia de la doctrina del secreto en relación con la regulación de las actividades de inteligencia utilizando fuentes abiertas y redes sociales en la Argentina. En el mes de abril de 2021 desde ICCSI enviamos una serie de pedidos de acceso a la información dirigidos a los ministerios o secretarías de seguridad de todas las provincias y de la CABA.

Allí solicitamos conocer, entre otras cuestiones, si esos organismos o las policías a su cargo realizan tareas de investigación y/o seguimiento en fuentes abiertas, quiénes y cómo las llevan adelante, qué capacitación reciben las personas involucradas, si los datos obtenidos se registran y almacenan, etc. Veintitrés jurisdicciones no respondieron el pedido de información, ni siquiera para negar el acceso. La única respuesta que obtuvimos fue de la Dirección de Inteligencia Criminal de la Policía de la Provincia de Entre Ríos, que nos informó que en esa provincia sólo se realizan requerimientos a las empresas prestadoras de servicios de Internet, telefonía o sitios web, siempre y cuando esto sea solicitado mediante un oficio judicial, y que para ello no cuentan con un software u otra herramienta especializada, sino que proceden de manera manual a cumplimentar una tarea puntual.

Ahora bien, como hemos mencionado, durante el 2020 se produjo un hecho poco común que brindó una oportunidad, una ventana epistémica[22], para asomarse a las discusiones sobre las facultades y límites del Estado en la utilización de este tipo de fuentes para la inteligencia criminal, así como a las confusiones que existen entre la inteligencia criminal y otras tareas realizadas por las policías.

La oportunidad fue una derivación de la decisión del Ministerio de Seguridad de la Nación de dar a conocer un proyecto para regular actividades policiales en fuentes digitales abiertas. Es probable que esto haya sido posible, es decir su discusión pública, porque las autoridades no encuadraban esas actividades como formas de la inteligencia criminal, sino como prevención policial.

El protocolo del Ministerio de Seguridad de la Nación

En abril de 2020 el Ministerio de Seguridad de la Nación (en adelante, el Ministerio) informó que, en el marco de las tareas de control de cumplimiento de las restricciones a la circulación impuestas para prevenir la difusión del virus Covid-19, estaba realizando tareas de *ciberpatrullaje*.

Ante las críticas realizadas por distintas organizaciones que enfatizaron la necesidad de regular estas actividades, el Ministerio puso en circulación un proyecto de protocolo y convocó a una mesa de discusión. Allí se presentaron distintas propuestas para mejorar el proyecto inicial. Finalmente, en junio de 2020 fue aprobada y publicada en el Boletín Oficial una nueva versión del protocolo, que incorporó algunas mejoras y precisiones, pero que en lo sustancial sigue arrastrando varios problemas.

22. En su trabajo sobre la regulación policial del narcotráfico en la provincia de Buenos Aires, Marcelo Sain denomina "ventana epistémica" a un suceso que brinda la oportunidad de asomarse, por un momento determinado, a lógicas que de ordinario permanecen opacas y son activamente ocultadas por los actores involucrados. En aquel caso, se trató del asesinato de Candela Sol Rodríguez ocurrido en 2011. El resquebrajamiento momentáneo del "doble pacto" entre policías y narcotraficantes a partir de ese hecho permitió acceder a información sobre el funcionamiento de algunas redes de ilegalidad en la zona noroeste del conurbano bonaerense (2015).

Junto con el primer proyecto, las autoridades dieron a conocer la normativa vigente en ese momento, que había sido aprobada en julio de 2018[23] por la anterior gestión. Era la primera vez que se hacía pública una regulación de este tipo. Se trataba de una comunicación de carácter general en la que el secretario de seguridad instruía a las áreas de *ciberdelito* de las fuerzas federales para "tomar intervención" en un conjunto definido de delitos, a través de "actos investigativos" que debían realizarse en sitios digitales de acceso público.

Por su nivel de generalidad, esta resolución no podía ser considerada un protocolo de actuación: no definía claramente las características de los "actos investigativos" ni los escenarios en los que podrían iniciarse. Por un lado, se infiere que podría tratarse de actuaciones sin orden ni control judicial ya que según el art. 2 una vez "reunidos los medios probatorios necesarios" se establecería el contacto con los funcionarios judiciales. Por otro lado, la definición acotada de los delitos enumerados parecía tener como objetivo impedir las tareas de vigilancia indiscriminada. Sin embargo, el carácter general y difuso de este instrumento generaba zonas grises al no aclarar qué tipo de decisión (y tomada por qué actor) es la que podría iniciar las intervenciones de las áreas dedicadas a los ciberdelitos. La resolución parecía una forma de dar cobertura a las tareas que las fuerzas ya venían llevando a cabo, más que un protocolo de actuación.

El proyecto de abril de 2020 fue presentado por el Ministerio como superador de esa resolución anterior, a la que debía derogar, ya que supuestamente especificaba y clarificaba lo allí dispuesto. No se ocultaba sin embargo que el motivo principal era contar con un instrumento para realizar acciones de control vinculadas a la pandemia, ya que en el art. 3 establecía: "La prevención policial del delito en el espacio cibernético procurará el conocimiento de posibles conductas delictivas cuyo acaecimiento sea previsible en función de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la pandemia declarada por la Organización Mundial de la Salud (OMS) en relación con el coronavirus Covid-19".

El proyecto definía las tareas de *ciberpatrullaje* como prácticas de monitoreo, observación y análisis de información de la actividad de las y los ciudadanos/as en las redes sociales para detectar hechos que configuren delitos, actividades que eventualmente pueden resultar criminales o aportar información sobre la comisión de delitos.

En los considerandos se explicaba que el *ciberpatrullaje* debía ser entendido como una técnica policial profesional y específica, la cual implicaba para su desarrollo el empleo de saberes y tecnologías tendientes a la recolección y análisis de información general y pública, obtenida de fuentes abiertas y digitales por personal calificado para dicha tarea, con la finalidad de identificar hechos, prácticas y eventos que afecten la seguridad interior, según establece

23. RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018.

la ley 24.059. Proponía su aplicación "para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad dependientes del Ministerio de Seguridad" mediante fuentes digitales abiertas (arts. 1 y 2).

Se establecía así una equivalencia con la tarea policial de patrullaje preventivo en las calles y el espacio físico. Esta asimilación entre las tareas de vigilancia general e inespecífica que los efectivos policiales pueden realizar en el espacio público, y las tareas de vigilancia en plataformas, redes sociales y otras formas de circulación de información basadas en Internet o en otras redes, se ve reforzada cuando el proyecto de protocolo intentaba especificar los delitos a perseguir.

Si bien por un lado hacía mención, como ya se dijo, a delitos "previsibles en función de la emergencia pública en materia sanitaria" (sin especificarlos), por otro lado, en el mismo art. 3 definía "como objeto de las tareas de prevención policial con uso de fuentes digitales abiertas, posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar acciones tipificadas penalmente". La detección de "posibles conductas delictivas" sin más especificación habilitaría a realizar prácticas de vigilancia masiva de las fuentes abiertas.

Todo lo que se produce en el espacio digital sería pasible de vigilancia y eventualmente persecución penal, ya que el mero uso de sistemas informáticos bastaría para activar el protocolo. Pretender "prevenir el delito" en el espacio digital de esta manera, implicaría que las fuerzas policiales monitoreen y vigilen de manera indiscriminada y sistemática las fuentes abiertas a la espera de detectar un delito o de que alguien exprese su intención de cometerlo.

En los últimos años, la idea de la "prevención situacional" en el espacio público fue ganando consenso entre quienes diseñan e implementan políticas de seguridad, lo que llevó a la expansión de la presencia policial en las calles, confiando en el potencial disuasorio de esa mera presencia. Si bien la eficacia de este tipo de patrullaje podría ser problematizada, lo relevante para plantear aquí es que si se asimila el *ciberpatrullaje* con el patrullaje preventivo en las calles, necesariamente hay que pensar en los efectos disuasivos que implican la presencia policial en las plataformas y redes sociales, y en qué significa esa disuasión (es decir, esa capacidad de evitar que se desplieguen ciertas conductas por temor a que sean percibidas por los efectivos policiales) en un ámbito que es básicamente una articulación de canales y medios de comunicación y expresión. La analogía entre patrullaje preventivo y *ciberpatrullaje* es engañosa y busca presentar a este último como una actividad distinta a la inteligencia criminal.

Lo que se desprendía de los arts. 2, 3 y 4 del proyecto de protocolo es que habilitaba a los organismos de las fuerzas de seguridad a buscar información en fuentes de Internet abiertas para detectar y alertar sobre la comisión de eventuales delitos. Esto no es *patrullaje*, sino tareas de inteligencia criminal que requieren de regulaciones particulares.

A partir de las críticas que recibió el proyecto original por habilitar una vigilancia masiva ilegal, se modificó la letra y en la versión final aprobada en junio[24] se puede leer que "la Secretaría de Seguridad y Política Criminal, dispondrá el procedimiento estandarizado y la definición de los indicadores delictivos que orientarán la actividad preventora de los cuerpos policiales y fuerzas de seguridad en el marco de la política criminal del Ministerio de Seguridad durante la emergencia pública en materia sanitaria establecida por Ley N° 27541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la pandemia declarada por la Organización Mundial de la Salud (OMS) en relación con el coronavirus Covid-19" (art. 4).

Es decir, se buscó limitar la habilitación a tareas de vigilancia indiscriminada introduciendo la idea de "indicadores delictivos" y poniendo en cabeza de la Secretaría de Seguridad (y no de los propios policías) la tarea de definirlos, aunque nuevamente sin especificar cómo se realizará esa definición.

Cabe señalar, finalmente, que tanto el proyecto original como el protocolo aprobado hacen referencia a que su vigencia se extiende mientras dure la "emergencia pública" por la pandemia. Esto, que algunos funcionarios/as presentaron como un atenuante en tanto el protocolo no sería un instrumento permanente, en realidad constituye otro problema porque vuelve a dejar en total incertidumbre qué sucederá con la regulación de estas actividades una vez superada la crisis sanitaria. Se debe avanzar entonces en la discusión de un marco normativo específico y permanente.

Mencionamos la experiencia de dicho protocolo a modo de ejemplo de las cuestiones que hacen al uso de fuentes digitales en el despliegue de la inteligencia criminal, tomando como positiva su discusión pública y los efectos que conllevó para acreditar todas las vacancias vinculadas a la temática y transparentar los puntos que deben acordarse para su regularización.

El ciberpatrullaje debe ser regulado como tarea de inteligencia criminal

Como se desarrolló en los capítulos anteriores, tanto las policías como otros actores están facultados para realizar tareas de inteligencia criminal, pero bajo ciertos límites y autorizaciones legales. Ni un protocolo ni una ley podrían autorizar una herramienta para realizar vigilancia indiscriminada sin hipótesis delictivas previstas y/o necesidades o sospechas sustanciales que justifiquen el inicio del ciclo de inteligencia criminal. Se encuentra prohibido lo que se conoce como "excursiones de pesca" para ver si alguien está cometiendo delitos en el entorno digital.

24. Resolución del Ministerio de Seguridad de la Nación Nº 144/2020. Boletín Oficial. Fecha: 31 de mayo del 2020. Disponible en el siguiente link. Última consulta: 16 de agosto del 2021.

Las definiciones del proyecto de protocolo que mencionamos sobre lo que no se puede hacer, como la "observación de individuos/as" era meramente retórica y técnicamente incorrecta. La habilitación era tan amplia que no había forma de que se restrigiera su uso frente a personas porque el objetivo del protocolo era justamente identificar autores/as de delitos y no realizar un análisis de posibles fenómenos criminales.

El marco conceptual y jurídico para analizar si son legales las tareas denominadas de *ciberpatrullaje* y para avanzar en una regulación de las actividades policiales de recolección de información en fuentes abiertas y redes sociales no es el de la prevención del delito, sino el de la inteligencia criminal. Por lo tanto, su regulación debe atenerse a la normativa sobre seguridad e inteligencia.

La cuestión central a definir es con qué alcance los organismos de seguridad pueden realizar actividades de inteligencia criminal a través de la vigilancia e inteligencia de fuentes abiertas (OSINT) y particularmente de medios sociales (SOCMINT). Es necesario que esta actividad sea regulada por ley para definir su alcance, herramientas tecnológicas permitidas y controles. Este es un debate que está pendiente en nuestro país, donde no hay nada regulado en este aspecto.

Asimilar la práctica de *ciberpatrullaje* al trabajo policial preventivo, tal como lo hacía aquel proyecto y quedó establecido en el protocolo publicado, trae una serie de problemas vinculados con los efectos de la vigilancia estatal indiscriminada sobre todas las personas: el monitoreo de las redes sociales por parte de las fuerzas de seguridad es un tipo de injerencia estatal excesiva en el espacio público, en la libertad de expresión y en la circulación de informaciones y opiniones, así como en la esfera de la intimidad.

La vigilancia permanente de las expresiones vertidas en el espacio público sin hipótesis delictiva previa y sin identificar qué o a quiénes se busca, tiene graves efectos sobre la libertad de expresión y en la circulación de informaciones y opiniones. Es lo que se conoce como *chilling effect,* o efecto disuasorio, que redunda necesariamente en el debilitamiento de una esfera pública amplia y plural.

El hecho de que toda la información que las personas colocan en sus redes sociales sea pasible de ser sometida a la vigilancia de las fuerzas de seguridad y posterior persecución penal es claramente violatorio de los estándares internacionales en la materia, ya que se ven vulnerados los derechos a la libre expresión, circulación, privacidad e intimidad, entre otros.

En síntesis, el *ciberpatrullaje* es un concepto técnicamente errado, que en realidad hace referencia a la búsqueda de información en fuentes digitales para la toma de decisiones en materia de política de seguridad, política criminal y persecución penal. Como tal, entonces, es una práctica que puede llevarse adelante bajo estrictos controles de legalidad, habilitaciones y limitaciones específicas que, como hemos visto, rigen a las actividades de inteligencia criminal.

Estas habilitaciones y limitaciones implican también la definición previa de una justificación argumentada sobre la necesidad de recolectar información sobre fenómenos o dinámicas delictivas específicas que orientan y limitan las intervenciones posibles en términos de tiempo y lugar (físico o virtual), excluyendo la posibilidad de la vigilancia inespecífica a la espera de la detección de delitos en general. Esto es, la justificación del ciclo de inteligencia criminal al que hemos hecho referencia previamente.

A su vez, si esas búsquedas en dichas fuentes de información se orientan hacia personas específicas y pueden afectar sus derechos constitucionales (incluso potencialmente) deben contar con una orden judicial y, cuando así sea necesario, realizarse en el marco de una investigación controlada desde las fiscalías y las judicaturas.

La perspectiva estatal que asimila las tareas de inteligencia criminal en fuentes abiertas y redes sociales con actividades policiales de prevención de delito, que no requieren en principio el mismo nivel de regulación y control porque se supone que son poco invasivas y gravosas, quedó así por el momento plasmada en el protocolo de actuación para el *ciberpatrullaje*. Esto es un síntoma más de la necesidad de clarificar discusiones, ordenar categorías y delimitar atribuciones y restricciones entre las tareas de prevención, investigación e inteligencia criminal. Esta publicación busca ser un aporte sustantivo para sentar las bases para las discusiones que vendrán.

Necesidades de cara a la regulación de la inteligencia criminal

Cada punto que hemos mencionado aquí demuestra lo incipiente que es la discusión sobre inteligencia criminal y el camino que hay que transitar aún en la materia. La conclusión principal es la necesidad de robustecer el campo teórico y regulatorio para empezar a perfilar prácticas democráticas y eficientes en todos los campos de aplicación de la inteligencia criminal.

Es por eso que, de ahora en adelante, es preciso afrontar un camino de desafíos escalonados para construir una doctrina de inteligencia criminal propia. Para ello consideramos necesario, en el largo, mediano y corto plazo, según corresponda:

→ Generar un marco conceptual preciso acerca de la inteligencia criminal que contribuya a definir sus objetivos y metodologías para impulsar mejoras en las discusiones y acuerdos al interior del Estado.

→ Regulación por ley de la actividad de inteligencia criminal para los ministerios de seguridad, las fuerzas policiales, los ministerios públicos fiscales y las fiscalías, tanto a nivel provincial como federal, con pautas de funcionamiento y límites claros al respecto. Urgen aquí su separación en relación a la inteligencia nacional y militar.

→ Creación de normativas, reglamentos y/o protocolos al interior de cada organización que permitan regular en forma detallada las obligaciones, límites y permisiones dentro de cada dimensión del ciclo de la inteligencia criminal.

→ Creación de normativa pertinente en torno a la exploración de las fuentes de información digitales para la inteligencia criminal y demás actividades estatales acordes a la Constitución Nacional, la ley de datos personales, los códigos procesales penales, entre otras normativas.

→ Conformación de cuerpos especializados e interdisciplinarios –policiales y civiles– que se aboquen a la actividad de inteligencia criminal y a la contrainteligencia criminal y que coordinen esfuerzos hacia el interior y exterior de las organizaciones.

→ Reformas al interior de las fuerzas de seguridad que permitan la profesionalización de las personas a cargo de la inteligencia criminal en sus diversas funciones: la seguridad pública, la política criminal y la persecución penal. Ello implica un debate serio en torno a la creación de las policías de investigaciones, diferenciadas de las policías abocadas a las actividades de prevención.

→ Actualizar la normativa pertinente a la ley de datos personales y al acceso a la información pública.

→ Modernizar las reglamentaciones del abordaje del delito en el espacio digital –y sus conceptualizaciones– y las técnicas de investigación especiales, profundizando el conocimiento del espacio digital y sus implicancias en la actualidad.

→ Mejorar los niveles de controles intraorganizacionales de la actividad de inteligencia criminal a partir de los órganos encargados de ello, como fortalecer los controles externos parlamentarios según la organización productora.

Palabras finales

Este documento resume sólo algunas de las ideas que fuimos construyendo para pensar alternativas a la realidad actual de la inteligencia criminal. Es una propuesta que requiere de mayor profundización. Sin embargo, nuestra intención no es agotar la discusión aquí, sino delimitar algunos de los apuntes a tener en cuenta para el momento del debate político que habrá que impulsar en materia de inteligencia criminal, su modernización y regulación.

Pretendemos colaborar para sacar del terreno opaco y engorroso en el que se suele ubicar a la inteligencia criminal y sus usos, para plantearla como una actividad esencial del Estado, para mejorar la toma de decisiones en materia de seguridad y política criminal. Esto requiere de limitaciones y controles rigurosos por el tipo de acciones que puede implicar.

Por ello, en esta ocasión buscamos dialogar con su definición, alcances, responsables, prohibiciones y habilitaciones a la par de brindar algunas ideas para orientar una metodología de trabajo que atienda a sus características y necesidades particulares.

Esperamos que este documento sea de utilidad para rediscutir la inteligencia criminal y, por supuesto, para rediscutirnos y pensarnos en forma permanente y hacia el futuro. Nos interesa la consolidación de nuestra democracia, donde la inteligencia criminal sólo tiene lugar si cumple funciones para mejorar la calidad de vida de las personas a través de impactos positivos en materia de criminalidad, seguridad pública y bienestar social.

Bibliografía y material consultado

Bibliografía y material consultado[25]

Alguna de esta bibliografía fue citada en concreto y otra ha favorecido al debate y la construcción de ideas sin ser citada. Las mencionamos ya que la naturaleza de este documento es de divulgación y con el fin de generar propuestas para la discusión.

- **Arias Pérez, José Enrique y Aristizábal Botero, Carlos Andrés.** (2011). El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. *Revista Semestre Económico*, 14 (28). Disponible en el siguiente **link**.

- **Asociación por los derechos civiles.** (2018). *Seguidores que no vemos. Una primera aproximación al uso estatal del open source intelligence (OSINT) y social media intelligence (SOCMINT).* Disponible en el siguiente **link**.

- **Binder, Alberto.** (2011). *Análisis Político Criminal. Bases metodológicas para una política criminal minimalista y democrática.* Editorial Ad Hoc, Buenos Aires, Argentina.

- **Cáceres, José Raúl.** (2001). *Inteligencia Estratégica. Visión proactiva y visión preventiva para la decisión.* Disponible en el siguiente **link**.

- **Carter, David.** (2009*). Law enforcement intelligence. A guide for State, local, and tribal law enforcement agencies.* Second Edition. U.S. Department of Justice, Estados Unidos. Disponible en el siguiente **link**.

- **Cea D'Ancona, Mercedes.** (1996). *Metodología cuantitativa: estrategias y técnicas de investigación social*. Síntesis Sociología, Madrid, España.

- **Centro de Estudios Legales y Sociales.** (2020). *Sobre el proyecto de protocolo de ciberpatrullaje*. Disponible en el siguiente **link**.

- **Coyne, John William y Bell, Peter.** (2011). Strategic intelligence in law enforcement: a review. *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 6, Nº 1, pág. 23-39. Editorial Routledge, Reino Unido.

- **Dammert, Lucía.** (2012). *Seguridad ciudadana y cohesión social en América Latina*. Colección de Estudios sobre Políticas Públicas Locales y Regionales de Cohesión Social Nº 3. Editorial Diputación de Barcelona (Oficina de Coordinación y Orientación del Programa URB-AL III).

25. Última consulta de los links: 16 de agosto del 2021.

- **Department of Defense USA.** (2010). *Joint Publication 1-02, Dictionary of military and associated terms*. Estados Unidos. Disponible en el siguiente **link**.

- **Department of the Army USA.** (2006). *Human Intelligence Collector Operations. Estados Unidos*. Disponible en el siguiente **link**.

- **Department of the Army of the United States.** (2005). *FM 3-19.13 Law enforcement investigations*. Disponible en el siguiente **link**.

- **Díaz Fernández, Antonio Manuel.** (2013). El papel de la inteligencia estratégica en el mundo actual. *Cuadernos de estrategia* Nº 162. pág. 35-66. Editorial Ministerio de Defensa de España, Instituto Español de Estudios Estratégicos.

- **Edwards, Lilian y Urquhart, Lachlan.** (2015). Privacy in public spaces: what expectations of privacy do we have in social media intelligence? *International Journal of Law and Information Technology* 24 (3). Disponible en el siguiente **link**.

- **Estévez, Eduardo.** (2015). Inteligencia criminal: una nueva disciplina para una antigua profesión. En Sergio Eissa (Compilador), *Políticas Públicas y Seguridad Ciudadana*. Pág. 229-243. Eudeba, Ciudad Autónoma de Buenos Aires, Argentina.

- **Estevez, Eduardo.** (2014). La inteligencia a partir del uso de Internet y las nuevas tecnologías. *Revista del plan Fénix*, Año 5, Nº 39, pág. 68-71. Editorial Voces en el Fenix, Facultad de Ciencias Económicas, Universidad de Buenos Aires, Argentina. Disponible en el siguiente **link**.

- **Estevez, Eduardo.** (Diciembre de 2014). Reformando la inteligencia policial en la provincia de Buenos Aires. *URVIO, Revista Latinoamericana de Estudios de Seguridad* Nº 15, pág. 71-84 (en línea). Editorial Flacso, Quito, Ecuador.

- **Evans, Glen.** (Diciembre de 2014). Limitaciones actuales del sistema de inteligencia argentino. *URVIO, Revista Latinoamericana de Estudios de Seguridad* Nº 15, pág. 10-26 (en línea). Editorial Flacso, Quito, Ecuador.

- **FAO.** (2004). *Guía Metodológica de Sistematización*. Honduras. Disponible en el siguiente **link**.

- **Gelli, María Angélica.** (2004). Constitución de la Nación Argentina. Comentada y concordada. Editorial La ley, Buenos Aires, Argentina.

- **ICCSI.** (2019). *¿Hay salida para la crisis del sistema de inteligencia?* Disponible en el siguiente **link**.

- **ICCSI.** (9 de junio de 2021). Seminario conjunto. Hacia un nuevo modelo de inteligencia estratégica. Disponible en **link**.

- **Jara, Oscar.** (1994). *Para sistematizar experiencias: una propuesta teórica y práctica*. Editorial Alforja, San José, Costa Rica.

- **Jimenez Villalonga, Rafael.** (2020). *El ciclo de Inteligencia: una explicación didáctica*. Global Strategy. Disponible en el siguiente **link**.

- **Jimenez Villalonga, Rafael.** (2018). *Tipos de inteligencia*. Global Strategy. Disponible en el siguiente **link**.

- **Jordan, Javier.** (2016). *Una revisión del ciclo de inteligencia.* Global Strategy. Disponible en el siguiente **link**.

- **Korkisch, Friedrich.** (2010). *NATO Gets better intelligence*. Institut für Außen- und Sicherheitspolitik, Viena, Austria.

- **Marradi, Alberto; Archenti, Nélida y Piovani Juan Ignacio.** (2007). *Metodologías de las ciencias sociales*. Emecé Editores, Buenos Aires, Argentina.

- **Martínez Elebi, Carolina.** Asesoramiento: Enrique Chaparro. Coordinación general: Beatriz Busaniche. (2018). Publicación realizada en el marco del proyecto sobre Seguridad, vigilancia y Derechos Humanos con apoyo de la Fundación Ford. Fundación Vía Libre.

- **Martínez Elebi, Carolina.** (2019). *Informe: Interceptación legal de las comunicaciones, hacia un sistema respetuoso de los DDHH*. Fundación Vía Libre.

- **National Defense Authorization Act for Fiscal Year 2006.** (2006). Public Law 109 - 163. United States. Government Printing Office. Estados Unidos. Disponible en el siguiente **link**.

- **National Security Agency Central Security Service.** (2021). FAQs (SIGINT). Disponible en el siguiente **link**.

- **Navarro Bonilla, Diego.** (2004). *El ciclo de inteligencia y sus límites.* Disponible en el siguiente **link**.

- **Office of the Director of National Intelligence (DNI).** (2013). US National Intelligence an Overview. Disponible en el siguiente **link**.

- **Omand David, Bartlett Jamie y Miller Carl.** (2012). Introducing social media Intelligence (SOCMINT). En *Intelligence and National Security*. Vol 27, Nº 6, pág. 801-823. Publicado por Routledge, Reino Unido.

- **Pérez Villalobos, María Concepción.** (2002). Derechos fundamentales y servicios de inteligencia. Grupo Editorial Universitario (GEU), Granada, España.

- **PNUD.** (2013). *Informe Regional de desarrollo humano 2013-2014. Seguridad ciudadana con rostro humano: diagnóstico y propuestas para América Latina.* Programa de las Naciones Unidas para el Desarrollo, Nueva York. Disponible en el siguiente **link**.

- **PNUD.** (1994). *Informe sobre desarrollo humano 1994*. Programa de las Naciones Unidas para el Desarrollo. Editorial Fondo de Cultura Económica, pág. 27-44, México D.F, México. Disponible en **link**.

- **Ratcliffe, Jerry.** (2007). Integrated intelligence and crime analysis: enhanced information management for law enforcement leaders. COPS-Police Foundation, Washington. Disponible en el siguiente **link**.

- **Richelson, Jeffrey.** (2008). *The US intelligence community*. Westview Press, Colorado.

- **Rosales Pardo, Ignacio Antonio.** (2005). La inteligencia en los procesos de toma de decisiones en la seguridad y defensa. *Cuadernos de Estrategia* Nº 130 (ejemplar dedicado a: El papel de la inteligencia ante los retos de la seguridad y la defensa internacional), pág. 37-64. Editorial Ministerio de Defensa: Instituto Español de Estudios Estratégicos.

- **Sain, Marcelo.** (2015). *La regulación del narcotráfico en la provincia de Buenos Aires*. Universidad Metropolitana para la Educación y el Trabajo, Ciudad Autónoma de Buenos Aires, Argentina.

- **Sautu, Ruth; Dalle, Pablo; Boniolo, Paula y Elbert, Rodolfo.** (2005). *Manual de metodología. Construcción del marco teórico, formulación de los objetivos y elección de la metodología*. Consejo Latinoamericano de Ciencias Sociales (CLACSO), Buenos Aires, Argentina. Disponible en el siguiente **link**.

- **Sistema Regional de Indicadores Estandarizados de Convivencia y Seguridad Ciudadana.** (2012). *Documento situacional sobre las fuentes de información en materia de convivencia y seguridad ciudadana en la República Argentina*.

- **Steele, Robert.** (1997). *Open source intelligence: what Is It? Why Is It Important to the Military?* Loch K. Johnson and James J. Wirtz (eds.). Roxbury, Estados Unidos.

- **Tudela, Patricio.** (2015). Análisis criminal, proactividad y desarrollo de estrategias policiales basadas en la evidencia. *Revista Criminalidad*, Nº 57. 1. Colombia.

- **Tudela, Patricio.** (2012). Análisis delictual y buenas prácticas en Sudamérica: lecciones y retos. Buenas Prácticas para el Análisis delictual en América Latina.

- **Ugarte, José Manuel.** (2019). Desarrollo, situación y probable evolución de la inteligencia criminal. Presentado en *X Congreso Latinoamericano de Ciencias Políticas*.

- **Ugarte, José Manuel.** (2001). *Legislación de inteligencia: especialización y control, legitimidad y eficacia*. Editorial Serviprensa, Guatemala.

- **Ugarte, José Manuel.** (2014). Panorama de la inteligencia criminal latinoamericana. Desarrollo, dilemas y dificultades. *Revista Urvio*, Nº 15, pág.41-54. ISSN: 1390-4299 (en línea). Flacso, Quito, Ecuador.

- **United Nations Office on Drugs and Crime.** (2011). *Criminal intelligence manual for managers.*

- **Wills, Aidan. (**2010). *Hacia un mejor conocimiento del control de la inteligencia. Kit de Herramientas – Legislando para el Sector de la Seguridad*. Centro de Ginebra para el Control Democrático de las Fuerzas Armadas (DCAF), Ginebra, Suiza.

Normativa vinculada

- Convención Americana de Derechos Humanos.
- Pacto Internacional sobre Derechos Civiles y Políticos.
- Declaración Universal de los Derechos Humanos.
- Convención contra la Tortura, y otros tratos o penas crueles, inhumanos o degradantes.
- Informe del Alto Comisionado de Naciones Unidas para los Derechos Humanos. Consejo de Derechos Humanos, 39º período de sesiones. A/HRC/39/29.
- Informe anual de la Comisión Interamericana de Derechos Humanos. 2020. Volumen II. Informe anual de la Relatoría Especial para la Libertad de Expresión.
- Ley 25520 Ley de Inteligencia Nacional.
- Ley 27126 Ley de Creación de la Agencia Federal de Inteligencia.
- Ley 24059 Ley de Seguridad Interior.
- Ley 23554 Ley de Defensa Nacional.
- Ley 27063 Código Procesal Penal de la Nación.
- Ley 27148 Ley Orgánica del Ministerio Público Fiscal de la Nación.
- Ley 27319 Ley Delitos Complejos. Investigación, Prevención y Lucha de los Delitos Complejos. Herramientas. Facultades.
- Ley 25326 Ley de Protección de Datos Personales.
- Ley 27275 Ley de Acceso a la Información Pública.
- Ley 27541 Ley de Solidaridad y Reactivación Productiva.
- Decreto 1311/2015 y anexos. Nueva Doctrina de Inteligencia Nacional.
- Decreto (DNU) 214/2020 Modificación a la Ley 2.520.
- Convenio sobre la ciberdelincuencia - Convenio de Budapest.
- Resolución 1617/2009. Ministerio de Justicia, Seguridad y Derechos Humanos. Estructura orgánica y funcional de la Policía de Seguridad Aeroportuaria. Anexo I.
- Resolución 144/2020. Ministerio de Seguridad de la Nación.
- Anteproyecto de ley elaborado por el Consejo Consultivo de la intervención de la Agencia Federal de Inteligencia (AFI).
- Proyecto de Ley de Seguridad Pública de la Provincia de Santa Fe.
- Proyecto de Ley del Sistema Policial de la Provincia de Santa Fe.


ICCSI