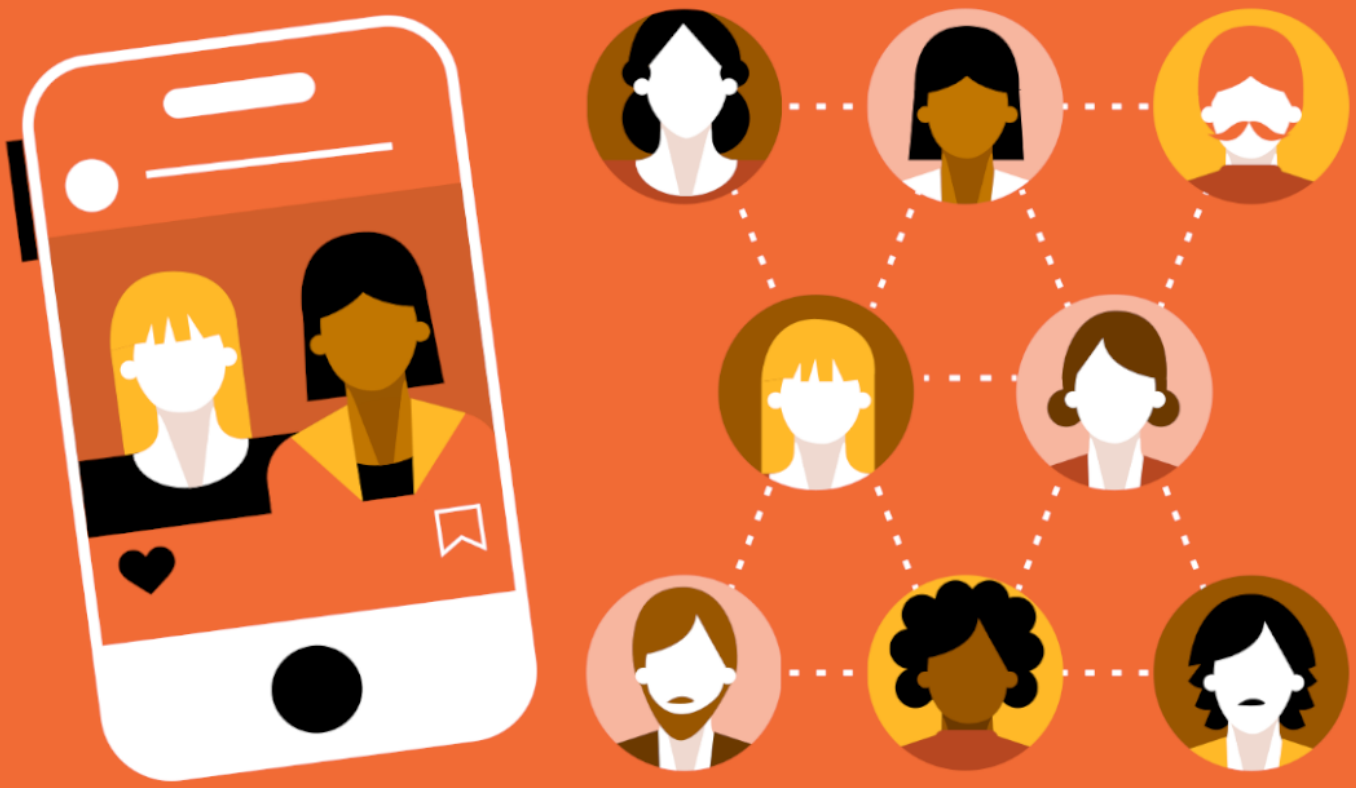
Ciberpatrullaje

LOS LÍMITES BORROSOS DE LA VIGILANCIA POLICIAL EN URUGUAY



datysoc.org

Ciberpatrullaje: los límites borrosos de la vigilancia policial en Uruguay

Por Patricia Díaz Charquero y Jorge Gemetto.

Una versión web de este informe puede visitarse desde este enlace.

Índice

1. Introducción

En junio de 2020, el periódico departamental Salto al Día publicó una entrevista al abogado Claudio Chaben, denunciante en un caso sobre incitación al odio en redes sociales. Si bien la nota fue dada de baja, está disponible aún en Internet Archive. El abogado afirmaba que, según una fuente del área de Delitos Informáticos de la Policía de Uruguay, la policía "*se encuentra tras los pasos de quienes publican, amenazan y expresan de forma escrita situaciones que pueden ser penadas por la ley*" y que tendrían identificados unos 2 mil grupos en redes sociales "*con características políticas, fundamentalmente de orientación de izquierda*". La nota también agregaba que a través de estas tareas de patrullaje en internet, tendrían a unas "*200 mil personas prácticamente identificadas por expresiones con tonos de aparente - delictivo* [sic]". Dudando de la veracidad de esta información, Gustavo Gómez, director de la organización de derechos humanos OBSERVACOM, presentó una solicitud de acceso a la información pública para saber si la policía uruguaya *"realiza un monitoreo sistemático de oficio en redes sociales para identificar expresiones de odio"*. Por su parte, el Ministerio del Interior desestimó la solicitud de Gustavo Gómez *"(...) en razón de que la información solicitada por el mismo tiene la calidad de 'reservada'(...)"*.

Más allá de la evidente violación a la Ley de Acceso a la Información Pública cometida por el Ministerio del Interior al declarar la reserva de la información sin cumplir con la obligación de probar el daño a la seguridad pública que se produciría en caso de entregarla, esta nota de Salto al Día y la declaración de reserva de la información solicitada por Gómez dejaron planteadas muchas interrogantes: ¿puede el Ministerio del Interior vigilar a los ciudadanos en redes sociales?, ¿puede seleccionar personas por su discurso en Twitter o Facebook y analizar sus posteos por considerarlos peligrosos o sospechosos?, ¿puede crear perfiles falsos para interactuar con personas en internet?, ¿tiene la capacidad instalada para hacerlo?, ¿este tipo de vigilancia está regulada?, ¿cuáles son sus límites?

Estas preguntas resultan muy oportunas en el contexto actual ya que, dentro de los planes de modernización de las fuerzas policiales de todo el mundo, existe una fuerte tendencia hacia la inclusión de este tipo de "ciberpatrullaje preventivo" en espacios digitales abiertos. Encontramos ejemplos claros de esta tendencia en Colombia, Argentina y España.

A través de este informe buscamos aportar elementos conceptuales para comprender qué es el "ciberpatrullaje", su relación con la inteligencia de fuentes abiertas (conocida como OSINT, acrónimo de *open-source intelligence*) y con la inteligencia de redes sociales (SOCMINT, acrónimo de *social media intelligence*), así como brindar recomendaciones de política pública desde la perspectiva de los derechos fundamentales.

Para lograr este objetivo, entre 2022 y 2023 realizamos las siguientes actividades: 1) elevamos una solicitud de acceso a la información pública al Ministerio del Interior de Uruguay, 2) mantuvimos entrevistas con informantes clave en la Fiscalía General de la Nación, 3) relevamos antecedentes y bibliografía sobre el tema, y 4) analizamos la legislación aplicable.

En la sección 2 de este informe se definen los conceptos de OSINT, SOCMINT y ciberpatrullaje, así como la relación entre ellos. En la tercera sección se analizan los riesgos para los derechos fundamentales que plantean las actividades de ciberpatrullaje. Para ello se examinan, en primer lugar, las diferencias existentes entre los espacios físicos y los digitales y, en segundo lugar, las diferencias entre las actividades de inteligencia policial y las actividades de instrucción procesal y de prevención del delito. En la cuarta sección se analiza el marco legal aplicable a las actividades de ciberpatrullaje en Uruguay, mientras que en la quinta sección se describe la situación del tema actualizada hasta mediados de 2023. Finalmente, se presentan recomendaciones para legisladores y para el Ministerio del Interior.

2. Definiendo OSINT, SOCMINT y ciberpatrullaje

La **inteligencia de fuentes abiertas (OSINT)** es aquella que utiliza un conjunto de técnicas y tecnologías para recolectar y analizar la información que se encuentra disponible públicamente, es decir, accesible para cualquier persona sin necesidad de contar con credenciales especiales de acceso de ningún tipo, en contraposición a información que se encuentra detrás de una capa de protección, como la de usuario y contraseña (*Seguidores que no vemos*, ADC, 2018). Entre estas fuentes se encuentran medios de prensa (como diarios, programas de radio y televisión y todo tipo de portal web), información oficial (como informes, datos demográficos, registros, debates legislativos, conferencias de prensa, discursos,

directorios y organigramas), información de portales académicos (como artículos, estudios y disertaciones, entre tantas otras publicaciones) y muchas otras fuentes.

La recolección de datos que se realiza más específicamente sobre plataformas digitales de comunicación social se conoce como **SOCMINT**. SOCMINT implica el uso de diferentes técnicas y tecnologías para la recolección, procesamiento y análisis de información de perfiles, fotos, videos, conversaciones, contactos, comentarios en blogs o prensa y, en general, todo tipo de información derivada de la interacción social en diversas plataformas o aplicaciones que incluyen contenidos generados por los usuarios (Twitter, Facebook, Instagram, TikTok, YouTube, LinkedIn, blogs, etc.). A pesar de que las técnicas de SOCMINT suelen ser asimiladas dentro del paraguas general de OSINT, existen grandes diferencias entre ambas prácticas. Veremos que uno de los desafíos centrales que enfrenta este tipo de prácticas es determinar dónde termina el espacio digital público y dónde comienza el espacio digital privado, lo cual tiene que ser debidamente diferenciado para garantizar regulaciones apropiadas con respecto al uso de esa información. Como afirma Eduardo Estévez, *"cuanto mayor sea el grado de intrusión en el espacio digital privado se requerirá una causa mayor, supervisión y control, legitimidad tanto de la agencia a cargo como de las competencias.*"

Tanto OSINT como SOCMINT se utilizan para obtener la información necesaria para planear, coordinar o ejecutar planes o estrategias que permitan conseguir ventajas, adelantarse a un hecho o a un enemigo. No se utilizan solamente para fines policiales o militares, sino que también son técnicas muy usadas en otros contextos. Por ejemplo, en la comunidad de seguridad de la información se usan para identificar riesgos en sistemas informáticos, mientras que organizaciones y activistas las usan para descubrir crímenes de guerra y violaciones de los derechos humanos.

Ciberpatrullaje es una expresión instalada en la jerga policial que implica el uso de SOCMINT en espacios digitales para prevenir el delito. Por ejemplo el Jefe de la Policía Colombiana (2021) explica qué es el ciberpatrullaje de esta forma: "*así como la Policía Nacional patrulla las calles, un barrio, una esquina verificando antecedentes, registrando personas, en fin, todo lo que hacemos en el mundo físico sin vulnerar ningún derecho para garantizar la seguridad pública y la convivencia, lo mismo sucede en ese mundo virtual, en ese espacio público virtual la autoridad tiene que ejercer ese servicio de vigilancia*". A su vez, el jefe de la Sección de Comercio Electrónico y Ciberdelincuencia de la Policía Nacional

española lo define de la siguiente manera: "*El ciberpatrullaje es una mezcla de técnicas, en su mayoría preventivas, con la finalidad de buscar actividad ilegal en la red y descubrir a los delincuentes. No consiste solo en el monitoreo de las redes sino también en la obtención y la recolección de información, el almacenamiento y el análisis del contenido que existe en las redes.*"

En los últimos años encontramos que existe una tendencia en países de América Latina de incluir las actividades de ciberpatrullaje en propuestas normativas relacionadas con prevención del crimen en espacios digitales. En estas propuestas normativas encontramos al ciberpatrullaje como una tarea policial prospectiva. Se trata de un monitoreo del espacio digital desarrollado con el fin de prevenir futuras acciones delictivas. Ciberpatrullar significa salir a "pescar" posibles delincuentes en las redes sociales sin una hipótesis delictiva definida. De acuerdo con los resultados de informes de diferentes países latinoamericanos (Argentina, Colombia, Brasil y México), este tipo de monitoreo continuo del espacio digital y perfilamiento de personas es utilizado, por ejemplo, para detectar posibles fraudes digitales, perfilar posibles integrantes de grupos radicales o redes de pedófilos, o inclusive para detectar noticias falsas (a pesar de que la Comisión Interamericana de Derechos Humanos ha expresado que esta práctica afecta gravemente la libertad de expresión), entre otros tantos focos de búsqueda posibles.

3. Ciberpatrullaje y derechos humanos

No es difícil detectar los riesgos que el concepto de ciberpatrullaje puede traer para el ejercicio de derechos fundamentales previstos en el Pacto Internacional de Derechos Civiles y Políticos, como la libertad de expresión, reunión y protesta, así como el derecho a la privacidad. El informe *Acerca de la Inteligencia Criminal en Argentina*, publicado conjuntamente por el Centro de Estudios Legales y Sociales (CELS), el Instituto Latinoamericano de Seguridad y Democracia (ILSED) y la Fundación Vía Libre, resume de esta forma el potencial impacto del ciberpatrullaje sobre los derechos humanos:

> *"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." (pág. 44).

A continuación presentamos dos aspectos que deberían tomarse en cuenta al momento de analizar las prácticas de SOCMINT desde una mirada de derechos humanos: 1) en los espacios en línea existen ciertas expectativas razonables de privacidad, incluso en las redes sociales "abiertas", y 2) el ciberpatrullaje no es una actividad de prevención del delito, sino inteligencia policial ejercida de forma ilegítima.

3.1. La peligrosa analogía entre el patrullaje en espacios físicos y el ciberpatrullaje

La analogía a la que recurren las autoridades policiales para justificar el concepto de ciberpatrullaje dista mucho de ser útil y entraña un enorme peligro conceptual. El supuesto de que las personas se comportan en línea de la misma forma que en las calles o espacios físicos públicos, concibiendo a internet de forma genérica como un espacio o fuente pública de información, es un mito a derribar.

En primer lugar, incluso en las calles existe una expectativa legítima de privacidad. Ciertas prácticas de vigilancia masiva, como el uso indiscriminado y sin controles de cámaras de vigilancia, el reconocimiento facial automatizado en tiempo real realizado en la vía pública, o la instalación de micrófonos en las calles para interceptar conversaciones, son prácticas ilegítimas con impacto en derechos fundamentales.

Cuando se aborda el tema de la privacidad en el espacio digital, de hecho resulta extremadamente complicado delimitar dónde termina la esfera privada digital y dónde comienza la pública. A continuación intentaremos dar una primera aproximación al tema, sin intentar agotarlo.

Por un lado encontramos que las plataformas sociales de internet, por razones comerciales, están diseñadas para establecer incentivos con el fin de que las personas compartan la mayor cantidad de información posible. Complementariamente, existen estudios que intentan explicar los motivos por los que las personas ofrecen más información o actúan con más frecuencia o intensidad en espacios digitales que en persona, y definen este fenómeno como el *efecto de desinhibición en línea*. Otros estudios postulan la *paradoja de la privacidad*, fenómeno por el cual las personas dicen que valoran fuertemente la privacidad, pero en su comportamiento ceden sus datos personales a cambio de muy poco o no toman medidas para proteger su privacidad. Finalmente, posiciones más recientes plantean una crítica al concepto de paradoja de la privacidad, ya que es imposible para cualquier individuo realizar una gestión de riesgos a escala masiva, por lo que el resguardo de la privacidad en el espacio digital es visto actualmente como un tema de gestión colectiva y no solo individual.

En ese mismo sentido, Edwards y Urquhart, en 2015, plantean que es necesario superar la idea de que las prácticas de SOCMINT no vulneran la privacidad de las personas porque las personas han elegido voluntariamente revelar su vida personal al mundo y, por lo tanto, se trata de fuentes "obviamente" públicas. Estos autores refutan esa aparente obviedad y plantean que existe una **razonable expectativa de privacidad** en dichos espacios debido a tres factores:

1. **Las personas no conocen realmente toda la información que están publicando en espacios digitales.** En estos espacios existe una gran cantidad de información que se puede utilizar con fines de inteligencia o de instrucción criminal y los titulares de esos datos no suelen ser conscientes de esa posibilidad. Entre este tipo de información se encuentran las redes de contactos (o el gráfico social de cada persona) y los metadatos de cada uno de los posteos, imágenes, videos, etc. Pensemos, por ejemplo, en la información que puede ofrecer una fotografía que se comparte en una red social o blog personal. La información que se encuentra en segundo plano en las fotografías es muy importante: calles, edificios, una laptop abierta, etc. A su vez, los metadatos Exif de una foto podrían llegar a revelar el nombre del autor, el dispositivo y sistema operativo con el que se tomó, si la foto fue editada, la geolocalización exacta de dónde fue tomada, la fecha y la hora. Si bien algunas redes

sociales, como Facebook y Twitter, eliminan estos metadatos de las fotografías, también cuentan con APIs a través de las cuales se pueden obtener otros tipos de metadatos de cada tuit o posteo.

2. **La información personal que se publica de forma abierta en espacios digitales no siempre es publicada por el titular de los datos**. Cualquier persona puede subir fotografías, videos o datos de un tercero, inclusive etiquetarlo o nombrarlo, aún si el titular de los datos no tiene cuenta en esa plataforma, por lo que no tiene el control sobre sus datos personales. A su vez, la información de las personas que han optado por cuentas "privadas" puede ser republicada por cualquiera de sus contactos.
3. **Resulta imposible realizar una correcta gestión individual de la privacidad online.** Esto es así porque las políticas de privacidad de cada plataforma son extensas, están escritas con términos técnicos y cambian constantemente. Además, dentro de una misma plataforma se aplican diferentes configuraciones de privacidad sobre diferentes piezas de contenido (fotos, posts, reels, contactos, grupos, etc). A su vez, cada plataforma tiene políticas de privacidad diferentes y las personas suelen habitar en decenas de plataformas.

Los autores concluyen su análisis expresando que:

> *"Puestos en conjunto, todos estos puntos muestran que, contrariamente a la creencia popular, el control sobre qué datos personales se hacen públicos en las redes sociales no es simplemente una cuestión de sencilla elección voluntaria. En consecuencia, la réplica común: 'si no quería que otra gente (como la policía) lo leyera, ¿por qué lo hizo público?' no es de hecho una pregunta sensata. Sostenemos que esto contribuye en gran medida al argumento de que* ***el material colocado en las redes sociales "abiertas" aún puede llevar consigo expectativas razonables de privacidad****."* (Edwards y Urquhart, 2015, págs. 15 y 16, traducción y resaltado nuestro).

3.2. No es prevención del delito, es inteligencia policial ilegítima

Estamos de acuerdo con Morena Schatzky y Agustina Del Campo cuando expresan, en un artículo de 2020, que **el concepto de ciberpatrullaje (basado en técnicas de inteligencia) confunde las tareas de inteligencia policial con las tareas de prevención e investigación criminal.** Las actividades de inteligencia policial tienen como objetivo la producción de conocimiento para asignar recursos y orientar la toma de decisiones en materia de políticas públicas sobre criminalidad y la seguridad. Esto sucede en un nivel de decisión general o de planificación, por lo que su objetivo no es la detección y represión de casos delictivos concretos, algo que suele estar expresamente prohibido en la mayoría de las leyes de inteligencia. Además, las actividades de inteligencia policial no pueden ser llevadas adelante por cualquier actor sino por aquellos habilitados específicamente para ello y bajo los estrictos controles y prohibiciones que las leyes de inteligencia establezcan. Es por eso que las actividades de SOCMINT no deberían aplicarse con fines de prevención del delito. En definitiva, reunir información de manera indiscriminada para, a posteriori, analizar si alguno de los datos obtenidos constituye un indicio de una actividad delictiva, es una práctica de vigilancia masiva lesiva de los derechos fundamentales.

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) expresa que, para que este tipo de actividad sea legítima, se **requeriría una orden de una autoridad judicial especializada basada en una hipótesis delictiva previa**, es decir, en indicios objetivos de determinado fenómeno criminal y un umbral de sospecha debidamente acreditado, con cierta delimitación espacial, temporal y/o personal, así como la justificación de la probabilidad de encontrar datos relevantes en la fuente abierta de que se trate. **Dicha orden judicial debería fundamentarse además en un análisis de los factores de proporcionalidad y necesidad.**

El problema que enfrentan varios países, entre ellos Uruguay, es la falta de una regulación específica sobre el alcance del uso policial de SOCMINT que cuente con un encuadre adecuado para delimitar los requisitos y controles específicos de este tipo de actividades en espacios digitales.

4. Marco legal aplicable en Uruguay

4.1. Ley N° 18.331 de Protección de Datos Personales

De acuerdo con el artículo 9 bis de la Ley N° 18.331 de Protección de Datos Personales, es legal el tratamiento de datos personales que se encuentren en "*fuentes públicas o accesibles al público*". Ese mismo artículo enumera cuáles fuentes deben considerarse públicas. La Unidad Reguladora y de Control de Datos Personales (URCDP) interpreta que internet no es, en sí misma y de manera general, una fuente pública. En su Dictamen N° 10/020, la URCDP expresa que: "*los datos personales que surjan en internet de personas físicas o jurídicas no son datos públicos o datos accesibles al público dado que Internet no es fuente pública de información (artículo 9° bis). Deberá analizarse cada página web para determinar si se encuentra dentro de alguno de los supuestos previstos en el artículo, y en su caso recabar el previo consentimiento del titular de los datos.*"

De esta forma, cuando las actividades de SOCMINT implican la recolección de datos personales en fuentes de internet, debe analizarse el tipo de fuente (artículo 9 bis) para detectar si se trata de un espacio digital público o privado, y cumplir con el principio de consentimiento informado si corresponde.

Pero este alcance limitado que la Ley de Protección de Datos Personales otorga al concepto de *fuentes públicas*, no es claro que sea aplicable al tratamiento de datos personales con fines de inteligencia y seguridad pública. Esto es así porque el artículo 3 literal B y el artículo 25 de la misma ley excluyen de su alcance el "*tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia*" siempre que "*resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas para la defensa nacional, la seguridad pública o para la represión de los delitos.*" El artículo 25 también establece que las bases de datos que se construyan deberán ser específicas y que los datos personales deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

Vale la pena aclarar que la protección de datos personales es un derecho fundamental (artículo 1), por lo que es posible esgrimir que existe una protección constitucional a este derecho. Sin embargo, en este caso, las bases y el

tratamiento de esos datos quedan fuera del control de la URCDP y no se requiere cumplir con los procedimientos u obligaciones formales previstos de manera general en la Ley N° 18.331. Queda así en manos del propio Ministerio del Interior determinar la oportunidad, la proporcionalidad y la necesidad para desplegar prácticas de SOCMINT. Se hacen necesarias, por lo tanto, protecciones legales más específicas.

4.2. Ley N° 19.293 - Código del Proceso Penal

Cuando en procesos de investigación criminal existen suficientes elementos de convicción para considerar que se ha cometido o pudiere cometerse un hecho punible, el artículo 208 del Código del Proceso Penal de Uruguay establece que el fiscal podrá solicitar al juez intervenir las comunicaciones mediante una orden judicial fundada y con determinadas características (análisis de necesidad y proporcionalidad y plazo acotado) bajo pena de nulidad.

La cuestión aquí es que no es claro que las actividades de SOCMINT puedan ser asimiladas al concepto de intervención de las comunicaciones previsto por el artículo 208 del Código del Proceso Penal, pensado para la intervención de fuentes cerradas, por lo que no existe legislación específica.

4.3. Ley N° 19.696 del Sistema Nacional de Inteligencia del Estado

El funcionamiento de los organismos de inteligencia en Uruguay se rige por la Ley N° 19.696 del año 2018 (Ley de Inteligencia) que crea el Sistema Nacional de Inteligencia del Estado (SNIE). El SNIE está integrado por la Secretaría de Inteligencia Estratégica de Estado (SIEE, órgano desconcentrado del Poder Ejecutivo), los órganos que desarrollan tareas de inteligencia y contrainteligencia de los Ministerios del Interior, de Defensa Nacional, de Relaciones Exteriores y de Economía y Finanzas, así como otros organismos del Estado que puedan contribuir al propósito del SNIE.

A pesar de que, de forma extraña, la ley no define la integración específica del SNIE, en el ámbito policial sería la Dirección General de Información e Inteligencia, a través del Departamento de Investigación e Inteligencia Criminal (artículo 93 de la Ley N° 19.670), la que realiza actividades de inteligencia policial.

4.3.1. Definición de fuentes abiertas y cerradas en la Ley de Inteligencia

En su artículo 3 literal H, esta norma define a las fuentes abiertas como *"aquellas de las cuales se puede obtener un determinado informe, sin más restricción que la tarea que demanda su obtención"*, a diferencia de las fuentes cerradas, a las que define como *"aquellas cuyo acceso es restringido y que para la obtención de la información es necesario el uso de medios y* ***procedimientos especiales****."* (Resaltado nuestro).

Esta distinción resulta fundamental, ya que indica que el régimen legal asignado a cada tipo de recolección de información depende del tipo de fuente. Veremos también la especial relevancia que otorga la Ley de Inteligencia al concepto de procedimientos especiales, ya que las operaciones de búsqueda de información que los involucren serán las que requerirán orden judicial.

Nótese que la definición de *fuentes* prevista en el artículo 3 literal H de la Ley de Inteligencia:

- No establece ninguna diferencia entre las plataformas digitales de comunicación social (SOCMINT) y las fuentes abiertas, por lo que no se contempla adecuadamente la expectativa razonable de privacidad que existe en este tipo de fuentes (ver apartado 3.1).
- No coincide con la definición de *fuentes públicas o accesibles al público* prevista en el artículo 9 bis de la Ley de Protección de Datos Personales (ver apartado 4.1).

4.3.2. La Ley de Inteligencia no distingue las tareas de instrucción y prevención del delito de las de inteligencia policial

El artículo 3 literal E de la Ley de Inteligencia define a la **inteligencia policial** como la *"actividad que comprende lo relativo a la obtención, procesamiento, análisis y distribución de información relativa a la prevención y eventual represión del delito común y el crimen organizado en su calidad de auxiliar de la Justicia, a través de la prevención y represión del delito"*.

Se trata de una definición que funde el concepto de inteligencia policial con las actividades de prevención del delito y de investigación criminal, generando una confusión peligrosa que implica un riesgo de expansión de la utilización de los informes y tecnologías de inteligencia a las actividades de prevención o represión y a la esfera de procesos penales (Rodrigo Rey, 2019).

En el artículo 7 numeral 1 de la Ley de Inteligencia encontramos que los organismos de inteligencia tienen prohibido, entre otras cosas, realizar por sí actividades de represión o investigación criminal, *"salvo que dicha actividad se encuentre dentro de sus cometidos legales específicos"*. Dado que las actividades de represión o investigación criminal forman parte de los cometidos de la policía nacional y también de la definición de inteligencia policial en la misma ley, tampoco es claro que podamos acudir a esta prohibición del artículo 7 para solucionar los problemas que genera la definición ambigua y problemática de inteligencia policial del artículo 3 literal E.

4.3.3. ¿Vigilancia en redes sociales sin orden judicial?

El artículo 20 de la Ley de Inteligencia requiere orden judicial para la obtención de información en fuentes cerradas en el marco de actividades de inteligencia y define el concepto de *procedimientos especiales* utilizado en el artículo 3 literal H.

> *"Artículo 20 (Autorización del Poder Judicial).-* ***Toda operación de búsqueda de información*** *que deba realizar cualquier órgano componente del Sistema de Inteligencia Estratégica de Estado,* ***involucrando procedimientos especiales*** *que puedan afectar la libertad y privacidad de los ciudadanos, deberá ser autorizada por el Poder Judicial. A tales efectos, serán competentes los Juzgados Letrados de Primera Instancia en lo Penal Especializados en Crimen Organizado. Las actuaciones serán de carácter reservado.*
>
> *(...)*
>
> ***Se entiende por procedimientos especiales de obtención de información, los que permiten el acceso a antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas****, que aporten antecedentes necesarios al cumplimiento de la misión operativa*

específica de cada agencia de inteligencia, tales como los siguientes procedimientos:

A) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas.

B) La intervención de sistemas y redes informáticos.

C) La escucha y grabación electrónica incluyendo la audiovisual.

D) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información." (Resaltado nuestro).

De esta forma, encontramos que el concepto de procedimientos especiales se relaciona únicamente con las fuentes cerradas, por lo que, de acuerdo a la Ley de Inteligencia, no sería necesario requerir autorización judicial previa para realizar SOCMINT.

El problema que genera el artículo 20 va más allá de omitir regular de forma diferenciada las actividades de SOCMINT. Según Rodrigo Rey, los procedimientos judiciales para la obtención de información en fuentes cerradas, que implican la intervención de las comunicaciones, tampoco se regulan con precisión, lo que impide un control judicial efectivo. Dicho autor expresa que:

"*Esto lleva a que sean las agencias administrativas quienes definan los eventos que dan lugar a la labor de inteligencia y no el legislador. En otras palabras, no existe un estándar legal mínimo de fundamentación y ese punto puede dar lugar a serias arbitrariedades. Tampoco se registran términos o plazos para la resolución y los posibles recursos y tampoco se prevé la posibilidad de prórroga, que justamente podría operar como control (efectivo, sobre los contenidos específicamente relevados y su pertinencia) sobre la ejecución de estos procedimientos.*"

Por su parte, el artículo 5 de la Ley de Inteligencia establece que la recolección y tratamiento de la información por parte de los órganos que integran el SNIE, entre ellos el Ministerio del Interior, se deberá ajustar a determinados principios como el de juridicidad, por el que se debe actuar en estricta observancia de la

Constitución, los tratados internacionales, las leyes y demás fuentes del ordenamiento jurídico, evitando en todo caso las actividades invasivas de la privacidad de las personas. De esta forma, existe un mandato genérico que obliga a respetar la privacidad (Ley N° 19.696, artículo 5 literal D) y otro mandato genérico de respetar los principios generales de protección de datos personales como derecho fundamental (Ley N° 18.331, artículo 1). Entendemos que estos mandatos genéricos no son suficientes y que las ambigüedades presentes en la Ley de Inteligencia dejan la puerta abierta para la implementación de actividades de ciberpatrullaje, es decir, de SOCMINT sin orden judicial y sin contar con una hipótesis delictiva previa, aduciendo tan solo fines genéricos de prevención del delito.

4.3.4. ¿Creación de perfiles falsos con fines de vigilancia sin orden judicial?

Otro problema grave que presenta la Ley de Inteligencia es la posibilidad de autorización de agentes encubiertos por la vía administrativa:

> *"Artículo 21* ***(Actuación encubierta)****.-* ***Los jerarcas*** *de los órganos que integran el Sistema Nacional de Inteligencia de Estado* ***podrán autorizar****, en forma escrita y debidamente clasificada,* ***que el personal*** *de su dependencia, en el cumplimiento de tareas específicas del servicio y en el marco de las disposiciones de esta ley,* ***oculte su identidad oficial y actúe en forma encubierta para la obtención de antecedentes e informaciones****. Dicha autorización habilitará la eventual emisión de los documentos necesarios para proteger la identidad del personal involucrado.*
>
> *Asimismo, dicho jerarca podrá autorizar la utilización de informantes, entendiéndose por informante a la persona que no siendo funcionario de un órgano de inteligencia proporciona información pertinente a los fines del Sistema Nacional de Inteligencia de Estado."* (Resaltado nuestro).

De esta forma, tampoco se requeriría de orden judicial para realizar actividades de SOCMINT acudiendo a la figura del *agente encubierto* del artículo 21. Queda así abierta la posibilidad de crear perfiles falsos en diferentes plataformas, acceder con una identidad encubierta a grupos de servicios de mensajería como Whatsapp o Telegram, interactuar directamente con las personas para obtener información, o simplemente acceder a información de perfiles privados por el solo hecho de ser aceptado como contacto.

Llama la atención la enorme diferencia que existe entre la figura del agente encubierto prevista por el artículo 21 de la Ley de Inteligencia y su homónima prevista en la Ley Contra el Lavado de Activos (Ley N° 19.574, artículo 64). Esta última se encuentra regulada de forma precisa, requiriendo orden judicial fundada, fijándose plazos máximos y estableciéndose la responsabilidad del agente tomando en cuenta los aspectos de proporcionalidad de su actuación.

4.3.5. Calificación genérica de reserva de la información de inteligencia

Otra cuestión que llama la atención es la calificación de reserva genérica que el artículo 29 de la Ley de Inteligencia prevé sobre las informaciones y los registros en poder de los órganos que conforman el Sistema Nacional de Inteligencia del Estado y de su personal. Este tipo de categorización genérica se aparta de los estándares internacionales que recomiendan reservar la información caso a caso siempre que se pruebe el daño al bien público tutelado. En este sentido, la Institución Nacional de Derechos Humanos ha sido categórica expresando que la Ley de Inteligencia del Estado *"no cumple con estos estándares en materia de tutela a los derechos de acceso a la información y protección de datos personales al debilitar el marco jurídico nacional consagrado por las Leyes 18.331 y 18.381 y sus Decretos Reglamentarios*." (INDDHH, pág. 27).

A su vez, el artículo 32 exime a los órganos de inteligencia de los controles de la Unidad de Acceso a la Información Pública y tampoco establece la obligación de informar sobre los procedimientos de obtención, recopilación, uso, traspaso, comunicación y resguardo de la información.

De esta forma, se bloquea la posibilidad de cualquier tipo de control ciudadano, no solo frente a las prácticas de SOCMINT que pueda estar realizando

la policía nacional, sino también sobre el destino y los usos de los datos personales almacenados con fines de inteligencia policial y sobre la obligación de eliminarlos una vez cumplidos los fines para los que fueron recolectados (artículo 25 de la Ley N° 18.331).

5. Situación actual

5.1. El Ministerio del Interior no cumple con la Ley de Acceso a la Información Pública

Resulta imposible conocer cuál es la situación del uso policial de SOCMINT en Uruguay, o incluso determinar de forma cierta si el Ministerio del Interior se encuentra desarrollando actividades de ciberpatrullaje, debido al incumplimiento sistemático de las normas de transparencia pasiva por parte de las autoridades.

En el marco de esta investigación, se realizó una solicitud de acceso a la información pública al Ministerio del Interior para conocer si existen dependencias dentro del organismo que realicen la recolección de datos personales en fuentes abiertas para la prevención y/o investigación de delitos, así como la existencia de protocolos relacionados con este tipo de actividades y contratos con empresas privadas que se dediquen a la recopilación y análisis de datos en fuentes abiertas. La solicitud se presentó el 13 de noviembre de 2022. Varios meses después de haber vencido el plazo legal para la respuesta y luego de ser intimado por la Unidad de Acceso a la Información Pública (UAIP) de Uruguay, el Ministerio declaró como reservada la información solicitada, utilizando criterios de clasificación de la información que la UAIP ya ha establecido como ilegales en varias oportunidades, como por ejemplo en el Dictamen N° 17/013 y en la Resolución N° 13 de 2022.

Vale la pena resaltar que el Ministerio del Interior de Uruguay se encuentra dentro de los organismos con mayores niveles de incumplimiento de la Ley de Acceso a la Información Pública, cuenta con uno de los puntajes más bajos en el ranking de transparencia de Uruguay y es uno de los organismos estatales que ha recibido mayor cantidad de demandas judiciales por parte de la sociedad civil en este sentido. Dos ejemplos recientes de estas demandas ocurrieron en ocasión de la negativa a responder sobre el registro de distintos procedimientos policiales, así como por el rechazo a brindar información sobre el software de reconocimiento facial adquirido por el organismo.

5.2. No existe regulación específica ni protocolos internos para actividades de OSINT/SOCMINT

A partir de una entrevista realizada para esta investigación con una fuente calificada en el ámbito de la Fiscalía General de la Nación, se constata que en el marco de las investigaciones criminales en nuestro país se recolecta información a través de diferentes técnicas OSINT y SOCMINT y que la figura del *agente encubierto* podría ser utilizada para la creación de perfiles falsos.

El informante calificado en la Fiscalía expresa que no existe regulación ni protocolos internos que pongan límites exactos, que establezcan procedimientos o que fijen mecanismos de rendición de cuentas ante el Poder Judicial para la recolección y tratamiento de información de fuentes abiertas. Resalta que hoy no existen garantías suficientes en cuanto a la aplicación de OSINT y SOCMINT por parte de la policía en Uruguay y que también hay otros problemas a tener en cuenta como la corrupción policial, la falta de preparación de los funcionarios policiales (y de la misma Fiscalía) al momento de manejar información y la falta de garantías para el acceso, manejo y cadena de custodia de la prueba digital. Afirma que son de público conocimiento algunos casos de filtraciones de información o de uso de la información del sistema policial para fines privados.

El Ministerio del Interior ha creado comisiones para tratar estos temas. Estas comisiones, sin embargo, son cerradas (aunque se ha invitado a funcionarios de Agesic y de la Fiscalía para integrarlas) y vienen trabajando principalmente en propuestas para el diligenciamiento de la prueba digital.

5.3. El Ministerio del Interior adquirió un software para el análisis de redes sociales

En la Memoria Anual del año 2020, el Ministerio del Interior declara que el Observatorio Nacional sobre Violencia y Criminalidad "*ha incorporado recientemente a su paquete de herramientas informáticas un software para el análisis de redes sociales (UCINET), lo que permitirá profundizar en los aspectos vinculares o relacionales de la criminalidad, un aspecto clave aún no abordado en nuestro país con la importancia que merece*."

UCINET es un software utilizado en apoyo a las actividades de OSINT y SOCMINT que sirve para el análisis y graficación de redes sociales. Incluye una

gran cantidad de medidas estadísticas e indicadores a partir de matrices de relaciones entre individuos o casos. Estos indicadores se utilizan para medir las relaciones de una persona dentro de la red, comprender el comportamiento de grupos y detectar personas influyentes. Vale la pena aclarar que el término *análisis de redes sociales* se utiliza de forma amplia, por lo que no refiere necesariamente a su uso en redes sociales digitales (como Twitter, Facebook o Instagram), sino a la detección de patrones y relaciones entre individuos de cualquier tipo de red (digital o no). Consultado sobre los fines y protocolos del uso de este software, el Ministerio del Interior de Uruguay declaró reservada la información.

Debido a la negativa del Ministerio del Interior a entregar la información pública que solicitamos, no hemos encontrado evidencia de que se haya contratado otro tipo de herramientas o servicios de SOCMINT para hacer barridos o monitoreo sistemático en páginas web, redes sociales, foros o grupos abiertos de chat con el fin de extraer información sobre temas, personas o agrupaciones de interés.

6. Recomendaciones

Desde Datysoc entendemos que es inaceptable la posibilidad actual o futura de que se someta a la ciudadanía a procesos de vigilancia masiva erosionando sus derechos fundamentales a la privacidad, la libertad de expresión, de reunión y de protesta. Urge establecer mecanismos legales y prácticas de transparencia que garanticen que los procedimientos policiales de SOCMINT cumplirán con el debido proceso y los estándares internacionales de legalidad, necesidad y proporcionalidad, prohibiendo bajo toda circunstancia el riesgo de vigilancia masiva e indiscriminada a la ciudadanía. A continuación elaboramos un conjunto de recomendaciones dirigidas al órgano legislativo y al Ministerio del Interior.

6.1. Recomendaciones para legisladores

Se recomienda:

- Revisar los aspectos más problemáticos (y posiblemente inconstitucionales) de la Ley N° 19.696 del Sistema Nacional de Inteligencia del Estado. En ese sentido, proponemos:

- Modificar la definición de inteligencia policial (artículo 3 literal E), diferenciándola claramente de las actividades de instrucción y prevención del delito y detallando de forma granular cuáles serían los objetivos exactos para los cuales podría recogerse la información.
- Modificar la definición de fuentes (artículo 3 literal H), diferenciando las plataformas digitales de comunicación social respecto de las fuentes abiertas. Recomendamos especialmente que se adopte la definición de *fuentes públicas o accesibles al público* del artículo 9 bis de la Ley N° 18.331 de Protección de Datos Personales.
- Incluir dentro del concepto de *procedimientos especiales* del artículo 20 aquellas actividades que impliquen el uso de SOCMINT en redes sociales u otros espacios digitales en los que haya una razonable expectativa de privacidad, de forma tal que queden incluidos dentro de aquellas situaciones que requieren una autorización judicial previa.
- Incluir de forma expresa, dentro de las prohibiciones previstas por el artículo 7, la prohibición de actividades de monitoreo sistemático e indiscriminado de la ciudadanía (vigilancia masiva).
- Requerir que la autorización judicial prevista en el artículo 20 inciso 1 contenga un estándar legal mínimo de fundamentación basado en factores de proporcionalidad y necesidad, duración máxima y determinación de los plazos para el cese de la actividad.
- Requerir autorización judicial fundada para la designación de agentes encubiertos, fijándose plazos máximos y la responsabilidad del agente tomando en cuenta los aspectos de proporcionalidad de su actuación.
- Adecuar el régimen de acceso y clasificación de información a los estándares internacionales plasmados en los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información.
- Establecer regulaciones específicas separadas para cada organismo integrante del SNIE que permitan diferenciar en forma detallada las obligaciones, límites y habilitaciones dentro de cada dimensión del ciclo de la inteligencia policial.

- Ante la negativa del Ministerio del Interior de informar a la sociedad civil sobre actividades de monitoreo en redes o actividades de SOCMINT con fines de prevención del delito, se recomienda a los legisladores realizar un pedido de informe parlamentario solicitando esta información.
- De constatarse el uso policial de SOCMINT, se recomienda:
    - Introducir las modificaciones necesarias a la Ley de Procedimiento Policial y al Código del Proceso Penal de modo que se garantice el debido proceso cuando el monitoreo de internet, aún sin intervención de comunicaciones, se torna en un mecanismo de vigilancia selectiva, así como la obligación de establecer protocolos de actuación.
    - Crear obligaciones legales para que el Ministerio del Interior haga pública información sobre el uso de tecnologías para la vigilancia y actividades de inteligencia. Algunos de los datos que deben publicarse incluyen el tipo de tecnologías usadas, el número de personas afectadas, los motivos del uso de las tecnologías, así como los responsables por su correcto uso.

6.2. Recomendaciones para el Ministerio del Interior

Se recomienda:

- Abstenerse de realizar actividades que impliquen SOCMINT en redes sociales sin autorización judicial.
- Cumplir con la Ley de Acceso a la Información Pública y con las resoluciones de la Unidad de Acceso a la Información Pública. La información que deba permanecer reservada por comprometer cuestiones operativas relacionadas con la seguridad pública o la lucha contra el crimen, debería detallarse especialmente, probando el daño a la seguridad pública en cada caso, y no indicarse de forma genérica, de acuerdo con lo establecido en los artículos 8 y 9 de la Ley de Acceso a la Información Pública y el artículo 25 de su decreto reglamentario.
- Evitar una cultura institucional de secretismo innecesario, impulsando procesos de transparencia, rendición de cuentas y participación ciudadana significativa que contribuyan al control ciudadano de las actividades de inteligencia y seguridad pública.

- Diseñar protocolos específicos y públicos para las actividades de SOCMINT, diferenciando el uso con fines de inteligencia del uso con fines de instrucción criminal y prevención del delito, y facilitando al mismo tiempo la evaluación sobre su necesidad y proporcionalidad.
- Publicar toda la información posible sobre contratos relacionados con la adquisición de tecnología que se usa para actividades de vigilancia, con el fin de facilitar el control ciudadano.

7. Créditos y agradecimientos

Texto: Patricia Díaz Charquero y Jorge Gemetto

Fecha de publicación: julio de 2023

Este informe fue publicado con el apoyo de Indela y del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo.