Ciberpatrullaje

AMPLIACIÓN DEL INFORME Y RESULTADOS DEL LITIGIO SOBRE VIGILANCIA POLICIAL EN INTERNET

datysoc.org

Ciberpatrullaje: Ampliación del informe y resultados del litigio sobre vigilancia policial en Internet

Por Patricia Díaz Charquero y Jorge Gemetto.

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

Índice

1. Introducción

El 17 de junio de 2024 el Ministerio del Interior (MI) cumplió la sentencia judicial que lo obligó a brindar información sobre actividades de ciberpatrullaje. Así culminó un proceso que comenzó en noviembre de 2022 cuando Datysoc realizó una solicitud de acceso a la información pública para conocer la naturaleza y el alcance de las actividades de inteligencia de fuentes abiertas (OSINT) realizadas por la policía uruguaya.

La información, que de acuerdo a la Ley de Acceso a la Información Pública (LAIP) el MI debió brindar en un plazo no mayor a 20 días hábiles, fue entregada más de un año y medio después, de forma parcial, y solo después de una sentencia judicial que no le dejó otra alternativa. La información brindada, aunque parcial, permite de todas maneras confirmar que la policía uruguaya se encuentra realizando actividades de vigilancia en Internet sin los protocolos y regulaciones necesarios para brindar garantías a la ciudadanía. Esta situación ya ha presentado consecuencias graves, como la detención y formalización de una persona por error y la vulneración de la privacidad de un periodista.

2. El arduo camino para ejercer el derecho de acceso a la información pública

La solicitud de acceso a la información realizada por Datysoc en noviembre de 2022 buscó obtener información de interés público sobre la recopilación de datos personales en fuentes abiertas en Internet por parte de la policía uruguaya. Se realizó en el marco de una investigación regional liderada por el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo. Esta investigación indagó sobre el uso de OSINT con fines de vigilancia en Argentina, Brasil, Colombia, México y Uruguay. El informe local de Uruguay fue publicado por Datysoc en julio de 2023, sin las respuestas del MI.

La inteligencia de fuentes abiertas (OSINT, acrónimo de *open source intelligence*) es aquella que recolecta y analiza información que se encuentra disponible públicamente. El uso de OSINT con fines de vigilancia en el ámbito específico de

las plataformas digitales de comunicación social se denomina SOCMINT (*social media intelligence*, o inteligencia en redes sociales). El uso policial de OSINT y SOCMINT en tareas de prevención e investigación de delitos se suele denominar "ciberpatrullaje", aunque se trate de una actividad de inteligencia que tiene diferencias importantes con el patrullaje policial en las calles. A diferencia de este, su objetivo principal es el procesamiento y análisis de información, se lleva adelante por agentes no identificados, y es común su aplicación sobre personas concretas que son objetivos de inteligencia.

Las preguntas que realizamos en la solicitud de acceso a la información fueron las siguientes:

1) Si existen dependencias dentro del organismo que realicen la recolección de datos personales en fuentes abiertas para la prevención y/o investigación de delitos, indicar cuáles dependencias. Indicar, además, la normativa, regulación y/o protocolo de actuación que sustenta dicha recolección.

2) Si se han realizado y/o aprobado estudios, regulaciones, propuestas de regulaciones, o documentos para los cuales se hayan recopilado datos en fuentes abiertas, indicar cuáles y facilitar enlace o archivo correspondiente.

3) Si se ha negociado y/o firmado contratos con empresas privadas que se dediquen a la recopilación y análisis de datos en fuentes abiertas (por ejemplo UCINET), indicar con cuáles, con qué fines y facilitar copia del contrato correspondiente.

El MI faltó a su obligación de brindar la información solicitada. Una vez vencido el plazo legal para hacerlo, la Unidad de Acceso a la Información Pública (UAIP) lo instó, en marzo de 2023, a entregar la información. Pasados más de tres meses desde la comunicación del organismo de control, el MI entregó una respuesta declarando toda la información reservada de manera genérica, sin cumplir con la obligación legal de justificar qué daño haría la entrega de la información a la seguridad pública. Tras un informe jurídico, la UAIP emitió su resolución final en noviembre de 2023. En ella, determinó que la reserva realizada por el MI no se ajustaba a los parámetros legales previstos en la LAIP, por lo que exhortó al MI a

desclasificar la información solicitada y a entregarla, aplicando el principio de divisibilidad si hiciera falta.

Si bien la resolución no fue recurrida por el MI, este continuó sin entregar la información, por lo que a Datysoc no le quedó otro camino para efectivizar el derecho de acceso que iniciar la acción ante el Poder Judicial reuniendo todos los antecedentes. En nuestra demanda argumentamos sobre los riesgos del ciberpatrullaje y la obligación del Estado de dar la información, más aún si esta es de interés público. Para esto nos apoyamos en la LAIP, la Constitución Nacional y tratados internacionales.

La respuesta del MI a la demanda judicial se limitó a repetir los argumentos utilizados en la reserva administrativa. A juicio del MI, "resulta casi de perogrullo que no puedan darse a conocer los medios y mecanismos que utiliza la policía para dar seguridad a sus ciudadanos". Detengámonos un momento en esta afirmación. Si se aceptara como válido un principio así, la actuación policial sería siempre absolutamente opaca a la ciudadanía, que quedaría desprotegida ante posibles abusos de autoridad o violaciones de derechos humanos.

La sentencia del juzgado de primera instancia, a cargo del Dr. Gabriel Ohanian Hagopian, tuvo lugar en abril de 2024. Nos dio la razón parcialmente y ordenó al MI responder las preguntas por sí o por no, permitiéndole omitir los detalles más específicos solicitados. Las implicancias de esta decisión serán analizadas más adelante en este informe. Desde Datysoc presentamos un recurso de apelación para que se atendiera a la totalidad de nuestra demanda, mientras que el MI también apeló la sentencia, insistiendo en la reserva total de la información.

Tras las respuestas de una y otra parte a las apelaciones, el Tribunal de Apelaciones en lo Civil de Cuarto Turno, integrado por el Dr. Guzmán López Montemurro, la Dra. Mónica Besio y el Dr. Alvaro França, emitió la sentencia definitiva en mayo de 2024 confirmando la sentencia de primera instancia.

Dado que vencido el plazo para cumplir la sentencia, el MI no había entregado la información, el juez envió una intimación al MI para ejecutar la sentencia. El 17 de junio de 2024, con un año y medio de demora, el MI entregó la siguiente información:

1) **SÍ** está realizando recolección de datos personales en fuentes abiertas para la prevención y/o investigación de delitos.

2) **SÍ** ha realizado y/o aprobado estudios, regulaciones, propuestas de regulaciones, o documentos para los cuales se hayan recopilado datos en fuentes abiertas.

3) **NO** ha negociado ni firmado contratos con empresas privadas que se dediquen a la recopilación y análisis de datos en fuentes abiertas.

3. Consideraciones sobre las interpretaciones judiciales problemáticas de la Ley de Acceso a la Información Pública

Dado que tanto el juzgado de primera instancia como el tribunal de apelaciones habilitaron al MI a responder las preguntas únicamente por sí o por no, hoy no es posible conocer detalles importantes incluidos en la solicitud de acceso a la información pública, como los siguientes:

- Qué dependencias del Ministerio realizan recolección de datos de fuentes abiertas.
- Qué normativa, regulación y/o protocolo de actuación sustenta dicha recolección de datos.
- Para la realización de qué estudios, regulaciones o documentos se han recopilado datos de fuentes abiertas.

Según los jueces que intervinieron, el MI no estaría obligado a responder estas preguntas que contienen un mayor grado de detalle, dado que podrían afectar la seguridad pública. Ni en la sentencia de primera instancia ni en la definitiva hay una justificación sobre esa opinión ni se indica de qué manera específica podría verse afectada la seguridad de la ciudadanía, sino que se basan en el

sobreentendido, a nuestro criterio equivocado, de que la divulgación de detalles sobre las prácticas policiales pone en peligro a la población. Las sentencias aducen que ese fue el criterio adoptado por la UAIP. Sin embargo, la resolución final de la UAIP, de noviembre de 2023, no hacía estrictamente tal afirmación, sino que, por el contrario, instaba al MI a realizar una versión pública de toda la información solicitada, aplicando el principio de divisibilidad, y entregar parte de la información en términos genéricos. El principio de divisibilidad, consagrado en el artículo 7 del Decreto N° 232/2010, reglamentario de la LAIP, establece que "si un documento contiene información que pueda ser conocida e información que debe denegarse en virtud de causa legal, se dará acceso a la primera y no a la segunda". Esto quiere decir que la información y documentos solicitados no deben negarse, incluso cuando contengan información que puede ser reservada, sino que el organismo debe entregarlos, editando o borrando de ser necesario los datos específicos cuya divulgación puede causar algún riesgo.

Desde Datysoc creemos que la interpretación jurídica adoptada por los jueces, en los hechos, le permite al Estado negar información detallada de sus prácticas aun si esta información es de interés público e incluso cuando el organismo estatal no haya justificado el daño potencial a la seguridad nacional que su divulgación traería. Recordemos que la LAIP establece que la información solo puede clasificarse como reservada "mediante resolución debidamente fundada y motivada, en la que se demuestre la existencia de elementos objetivos que permitan determinar que la divulgación de la misma genera un riesgo claro, probable y específico de daño al interés público protegido".

Tal como fundamentamos en nuestra demanda y en el recurso de apelación, la información solicitada en este caso reviste un alto interés público dado que refiere al uso de tecnologías y técnicas de recolección de datos personales con fines de vigilancia potencialmente lesivas de las garantías civiles. Aporta a que la sociedad en su conjunto pueda conocer las políticas públicas llevadas adelante por el MI en un área sensible para el mantenimiento de la democracia como es la seguridad pública. Las herramientas informáticas de recolección de datos en fuentes abiertas para la prevención, investigación y represión del delito aumentan de manera sustancial la capacidad de vigilancia del Estado sobre las personas, lo que demanda una mayor transparencia en su uso y aplicación. Este aumento de la capacidad de vigilancia no puede pasar por fuera del escrutinio público teniendo

en cuenta, como veremos más adelante, los riesgos que su uso indebido supone para los derechos humanos, incluyendo el derecho a la privacidad, a la libertad de expresión y de reunión, y el derecho de las personas a no ser detenidas arbitrariamente.

Vale la pena tener en cuenta que nada de la información solicitada al MI por Datysoc implica acceder a información específica sobre operativos policiales pasados o futuros. La información que pedimos refiere al funcionamiento y gestión de la administración pública. Se trata de un principio de la administración pública y del orden democrático conocer de primera mano y por parte de las autoridades qué acciones desarrolla cada dependencia del Estado y bajo qué reglas. Y en un contexto en el que la incorporación de tecnologías de la información por parte del Estado es cada vez más corriente, este principio incluye conocer qué tipo de herramientas usa el Estado, cómo se almacenan los datos personales de la ciudadanía, cuánto cuestan las herramientas utilizadas, cuál es la finalidad declarada para justificar su adquisición o uso, qué reglas existen para su uso, por cuánto tiempo se contratan, quiénes son los titulares de las empresas proveedoras, entre otros aspectos.

Más allá de los problemas mencionados, la decisión judicial tiene otros aspectos que son positivos. Ratifica que el MI no tiene la potestad de declarar reservada, de manera indiscriminada, todo tipo de información sobre su accionar. Esto es lo que el MI viene haciendo sistemáticamente, en los últimos años, en respuesta a las solicitudes de acceso a la información pública realizadas por medios periodísticos, organizaciones de la sociedad civil y ciudadanos particulares. Ante los pedidos recibidos, el MI cita dos resoluciones dictadas por el propio ministerio en julio de 2012 que declaran reservada de forma genérica toda la información relativa a la actividad policial. Esas resoluciones fueron observadas en reiteradas ocasiones por la UAIP y vienen siendo desestimadas por la Justicia en distintos fallos judiciales. Entre estos antecedentes se encuentra la sentencia que obligó al MI a brindar información sobre el uso policial de tecnologías de reconocimiento facial automatizado, tema que desde Datysoc hemos tratado en profundidad en nuestra publicación sobre los resultados del juicio sobre uso policial del reconocimiento facial automatizado en Uruguay.

A pesar de las observaciones de la UAIP y de las sentencias judiciales que reafirman esta cuestión, el MI sigue negando rutinariamente la información que la ciudadanía le solicita. De esta manera, pone obstáculos a la concreción del derecho fundamental de las personas al acceso a la información pública. Dado que no todos los peticionantes tienen el tiempo ni los recursos necesarios para afrontar un juicio contra el MI, muchas veces la información no es entregada nunca y la solicitud queda en la nada. Recalcamos que la transparencia de la función administrativa de los organismos públicos es un principio básico de cualquier sociedad democrática.

4. Análisis de las respuestas entregadas por el Ministerio del Interior

4.1. El MI realiza actividades de ciberpatrullaje para la prevención y/o investigación de delitos

La primera respuesta confirma que el MI lleva a cabo en la actualidad la recolección de datos personales en fuentes abiertas en el marco de tareas de prevención e investigación de delitos. Esto es algo que ya se podía deducir en 2022, cuando realizamos la solicitud de acceso a la información pública, en base a varios indicios. Uno de ellos era la publicación en la Memoria Anual del año 2020 de un apartado relativo a la compra del software UCINET, herramienta que sirve como apoyo para tareas de OSINT. A esto se sumaba una nota de prensa de junio de 2020, publicada en el medio "Salto al día" (y luego retirada), donde se afirmaba que el área de Delitos Informáticos de la Policía tendría identificados alrededor de 2.000 grupos en redes sociales "con características políticas, fundamentalmente de orientación de izquierda", en los que podría haber "más de 200 mil personas prácticamente identificadas por expresiones con tonos de aparente – delictivo". Esta afirmación preocupante nunca fue confirmada, pero despertó una solicitud de acceso a la información pública por parte de Gustavo Gómez, director de Observacom, para conocer si la policía uruguaya realizaba un monitoreo sistemático en redes sociales para identificar expresiones de odio. El MI desestimó la solicitud de Gustavo Gómez, clasificando la información solicitada como reservada.

Con posterioridad a nuestra solicitud de 2022, nueva información hizo más evidente que la policía realiza ciberpatrullaje con fines diversos.

En marzo de 2024 el periodista Eduardo Preve denunció públicamente que el MI había montado una investigación para determinar el origen de sus fuentes de información en un caso periodístico resonado. De acuerdo a informes de prensa (como este y este), el Ministerio analizó el perfil, los seguidores, fotografías y publicaciones en las cuentas de Instagram y Twitter del periodista. El caso despertó preocupación al revelar el impacto que un uso indebido de técnicas de OSINT por parte de la policía puede tener en el ejercicio de la libertad de expresión y de prensa.

En abril de 2024, el director nacional de la policía, José Azambuya, afirmó públicamente que la policía estaba monitoreando las redes sociales para investigar y prevenir peleas callejeras. Días antes se había producido un enfrentamiento entre grupos de adolescentes frente a un centro comercial y los medios de prensa habían atribuido el hecho a convocatorias realizadas en plataformas en línea. Según lo informado por la propia policía, personal de la Dirección de Inteligencia y de Investigaciones de la Jefatura de Montevideo estaban abocados a este monitoreo, buscando mensajes donde se convocara a nuevos enfrentamientos.

En el marco de esas tareas, se produjo la detención y formalización de adolescentes en base a informes de inteligencia de la policía. La familia de uno de los adolescentes detenidos denunció que su detención se produjo por el simple hecho de que su nombre era similar al nombre de perfil de otra persona involucrada en incidentes. Un periodista que investigó el hecho advirtió asimismo a las autoridades del MI que se habían equivocado de persona.

Estos ejemplos muestran la importancia crucial de contar con límites, normas y protocolos claros para el uso policial de técnicas de inteligencia en fuentes abiertas. El uso de técnicas de ciberpatrullaje, sin orden judicial y sin control, por parte de la policía, pone en riesgo derechos fundamentales como la libertad de expresión, la libertad de reunión e incluso el derecho de las personas a no ser detenidas arbitrariamente.

4.2. El MI ha realizado estudios, regulaciones o documentos para los cuales recopiló datos en fuentes abiertas

Esta respuesta del MI revela que el uso de inteligencia en fuentes abiertas es una práctica extendida que va más allá de las tareas de investigación y prevención, utilizándose de manera más amplia en documentos internos. Lamentablemente, la sentencia judicial ha impedido tener más detalles de qué tipos de documentos realiza el MI en base al monitoreo de plataformas de Internet, lo que habría sido de gran utilidad para tener un panorama más claro del uso policial de estas técnicas de vigilancia.

No se comprende el criterio del juzgado de primera instancia y del tribunal de apelaciones de negar la posibilidad de conocer los contenidos o, al menos, obtener los nombres, títulos o denominaciones de los reglamentos o estudios internos relacionados con las actividades de ciberpatrullaje que efectúa el MI. Conocer qué tipo de protocolo efectivamente existe o qué estudios internos se han realizado, puede resultar especialmente ilustrativo para entender qué actividades desarrolla la policía y si el organismo ha creado sus propios límites y responsabilidades sobre sus actividades de ciberpatrullaje (algo deseable aunque totalmente insuficiente en términos de garantías). Lo que no es entendible es cómo el hecho de dar a conocer a la ciudadanía siquiera los nombres o titulares de protocolos o estudios pueda vulnerar de alguna forma a la seguridad pública.

4.3. El MI afirma que no ha negociado ni firmado contratos con empresas privadas que se dediquen a la recopilación y análisis de datos en fuentes abiertas

La respuesta negativa a la tercera pregunta nos sorprendió. Como ya hemos dicho, en 2020 el MI adquirió UCINET, un software que sirve para el análisis y graficación de interacciones sociales. La adquisición de UCINET, software de la empresa privada Analytic Technologies, implica necesariamente que se ha firmado algún tipo de contrato con la compañía, dado que no se trata de software libre o de código abierto, sino de un software privativo cuya compra implica el establecimiento de un acuerdo de licencia de uso.

UCINET se utiliza para medir las relaciones de determinadas personas dentro de una red, comprender el comportamiento de grupos y detectar personas influyentes. Si bien sirve para detectar patrones y relaciones en distintos tipos de red (no únicamente en plataformas digitales como Instagram, Facebook, Twitter o TikTok), y si bien el MI afirmaba en 2021 que todavía no lo estaba usando en esas plataformas, su uso como apoyo para actividades de SOCMINT es ampliamente difundido. La respuesta negativa del MI a esta pregunta, por lo tanto, ameritaría una explicación.

Lo que parecería quedar descartado, afortunadamente, es la existencia de contratos en los que se tercericen en empresas privadas las tareas de análisis de datos personales de la ciudadanía.

5. Algunas conclusiones

En nuestro informe sobre ciberpatrullaje de julio de 2023 analizamos el marco legal aplicable y encontramos que la Ley N° 19.696 que regula el Sistema Nacional de Inteligencia del Estado (SNIE) confunde las tareas de instrucción y prevención del delito con las de inteligencia policial y habilita la vigilancia en redes sociales y la creación de perfiles falsos con fines de vigilancia sin orden judicial. También encontramos que la definición de fuentes abiertas que establece la Ley del SNIE incluye a las redes sociales, mientras que la Unidad Reguladora y de Control de Datos Personales (URCDP) establece que estas no podrían considerarse fuentes abiertas sin violentar el derecho humano a la protección de datos personales. Este último es uno de los varios argumentos que nos permite concluir que el ciberpatrullaje sin control judicial no cumple con estándares básicos de necesidad y proporcionalidad, y que no se trata de una actividad de prevención del delito, sino que constituye lisa y llanamente una actividad de inteligencia policial ilegítima.

La presente demanda nos permitió confirmar que el MI se encuentra efectivamente haciendo tareas de ciberpatrullaje sin un marco normativo que ofrezca garantías. De lo relevado hasta el momento, no se desprende que el MI tenga los recursos ni las capacidades para realizar un monitoreo de plataformas digitales en gran escala. El escenario más plausible es el de la existencia de personal dedicado a patrullar las redes en situaciones puntuales o con objetivos

específicos. Estas actividades se hacen sin una normativa que garantice los derechos de las personas cuyos datos personales están en juego. Los casos recientes que reseñamos en este informe, que incluyen la investigación inapropiada a un trabajador de prensa y la detención por error de un adolescente, ponen de relieve la necesidad urgente de establecer límites al monitoreo de la actividad de las personas en Internet y de construir protocolos para que la policía proceda adecuadamente en los casos muy específicos que ameritan procedimientos de ese tipo.

Los nuevos hallazgos confirman las preocupaciones planteadas por Datysoc en nuestro informe de 2023. Tal como dijimos en aquel momento, y más aún a la luz de la nueva información, resulta cada día más urgente establecer normas que regulen estas prácticas, así como obligaciones de transparencia que garanticen que los procedimientos policiales cumplen con el debido proceso y los estándares internacionales de legalidad, necesidad y proporcionalidad, prohibiendo bajo toda circunstancia la vigilancia masiva e indiscriminada a la ciudadanía.

Desde Datysoc seguimos poniendo sobre la mesa la necesidad de introducir modificaciones legales y transformar las prácticas del MI. Transcribimos a continuación nuestras propuestas, ya presentadas en trabajos previos.

5.1. 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 abiertas (artículo 3 literal H), diferenciando las plataformas digitales de comunicación social respecto de otras 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, aun 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.

5.2. 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.

6. Documentos del litigio

- Solicitud de acceso a la información pública realizada por Datysoc el 13 de noviembre de 2022: https://datysoc.org/wp-content/uploads/2023/07/Ciberpatrullaje-Solicitud-de-Acceso-a-la-Informacion-Publica-al-Ministerio-del-Interior.pdf
- Resolución del 1 de marzo de 2023 de la UAIP exhortando al MI a responder la solicitud: https://datysoc.org/wp-content/uploads/2023/07/Ciberpatrullaje-Resolucion-UAIP.pdf
- Respuesta del MI del 23 de junio de 2023 declarando reservada la información solicitada: https://datysoc.org/wp-content/uploads/2023/07/Ciberpatrullaje-Respuesta-del-Ministerio-del-Interior-a-Solicitud-de-Acceso.pdf
- Resolución final de la UAIP, del 3 de noviembre de 2023: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Resolucion-final-UAIP-noviembre-2023.pdf
- Demanda de acceso a la información pública, iniciada el 22 de marzo de 2024: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Demanda-Acceso-Informacion-Publica-Diaz-c-MI.pdf
- Contestación del MI a la demanda: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Contestacion-demanda-Ministerio-Interior.pdf
- Sentencia de primera instancia del juez Gabriel Ohanian Hagopian (9 de abril de 2024): https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Sentencia-de-Primera-Instancia.pdf
- Recurso de apelación de Datysoc: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Recurso-de-Apelacion-Datysoc.pdf
- Recurso de apelación del MI: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Recurso-de-apelacion-del-Ministerio-del-Interior.pdf

- Contestación de Datysoc a la apelación del MI: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Contestacion-de-Datysoc-a-la-apelacion-del-MI.pdf
- Contestación del MI a la apelación de Datysoc: https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Contestacion-del-MI-a-la-apelacion-de-Datysoc.pdf
- Sentencia definitiva del tribunal de apelaciones (6 de mayo de 2024): https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Sentencia-Definitiva-Segunda-Instancia.pdf
- Intimación del juez al MI para el cumplimiento de la sentencia (17 de junio de 2024): https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Intimacion-al-MI-para-el-cumplimiento-de-la-sentencia.pdf
- Cumplimiento de la sentencia (17 de junio de 2024): https://datysoc.org/wp-content/uploads/2024/06/Ciberpatrullaje-Cumplimiento-de-la-sentencia.pdf

7. Créditos y agradecimientos

“Ciberpatrullaje: Ampliación del informe y resultados del litigio sobre vigilancia policial en Internet” es una publicación de Datysoc.

Datysoc
LABORATORIO DE
DATOS Y SOCIEDAD

Texto: Patricia Díaz Charquero y Jorge Gemetto.

Abogado litigante: Matías Jackson.

Fecha de publicación: julio de 2024.

Este informe fue publicado con el apoyo de Indela y del Fondo de Respuesta Rápida de Derechos Digitales.

INDELA

FONDO DE
RESPUESTA
+ RÁPIDA
para la protección de derechos
digitales en América Latina