¿Ciberpatrullaje o inteligencia? - CELE

Mmdg ⋮ 15-19 minutes ⋮ 10/8/2020

Marco normativo y grises en una discusión que impacta directamente en nuestros derechos humanos.

El pasado 23 de julio, la Agencia Argentina de Acceso a la Información Pública (AAIP), Autoridad de Control de la Ley Nº 25.326 de Protección de los Datos Personales, sugirió al Ministerio de Seguridad de la Nación la **suspensión de la aplicación del Protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas** (en adelante, "el Protocolo") hasta tanto se revise nuevamente su adecuación a la normativa vigente en materia de protección de datos personales. Pasaron más de dos meses desde esa Nota y aún se desconoce si su implementación sufrió algún tipo de revisión.

El Protocolo, aprobado a fines de mayo de este año por la Resolución Nº 144/2020 del Ministerio de Seguridad de la Nación en el marco de de la emergencia pública en materia sanitaria establecida por Ley N° 27.541 y ss., en relación con el coronavirus COVID-19, . establece los *"principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad dependientes del Ministerio"*. El Protocolo renueva una política de Estado pre-existente y arrastra una discusión sobre la legalidad, proporcionalidad y necesidad de este tipo de prácticas estatales conocidas en la jerga como Open Source Intelligence (OSINT) y Social Media Intelligence (SOCMINT).

Los diferentes métodos de inteligencia sobre fuentes abiertas se han ido adaptando a medida que la tecnología ha ido evolucionando. Previo a la aprobación del Protocolo, existía un documento muy similar adoptado por la ex Ministra de Seguridad, Patricia Bullrich, que salió a la luz recién en abril de 2020, cuando la Ministra Frederic encomendó a las fuerzas de seguridad a buscar cualquier tipo de regulación que le permita monitorear la información en línea a fin de "medir el humor social".

Si bien la AAIP sugirió la suspensión del Protocolo por falta de adecuación a la normativa de protección de datos personales (que no es poca cosa viniendo de un órgano estatal), el Protocolo levanta otra discusión relativa al encuadre debido a estas actividades: ¿son tareas de prevención del delito o tareas de inteligencia? Atento al impacto de estas prácticas en nuestros derechos fundamentales, en particular la afectación a los derechos de libertad de expresión y privacidad, es necesario que la naturaleza jurídica de la actividad esté claramente establecida. En cualquier caso, ha de estar claramente estipulado el mecanismo de supervisión y control sobre estas herramientas, tanto en el orden administrativo como en el orden judicial. Permitir -o, peor aún, naturalizar- que los organismos estatales recaben, sistematicen, monitoreen, y utilicen información publicada en Internet sin ningún tipo de rendición de cuentas, por el solo hecho de obtenerlas de fuentes abiertas, supone enormes riesgos para el ejercicio de derechos humanos en internet y para la democracia.

Marco jurídico: ¿inteligencia disfrazada de vigilancia?

La inteligencia de fuentes abiertas (OSINT) "e*s la práctica que conlleva el uso de un conjunto de técnicas y tecnologías que facilitan la recolección de información que se encuentra disponible públicamente, como pueden ser textos, imágenes, videos, audios, e incluso datos geoespaciales. Recién en el momento que a dicha información se le encuentra una utilidad o propósito, y es asignada a una acción concreta, pasa entonces a convertirse en inteligencia propiamente dicha"*. (1)

Las prácticas de OSINT y SOCMINT existen desde hace décadas y los debates en torno a su legalidad están más vigentes que nunca. A comienzos de este año, a raíz del escándalo desatado por las denuncias de escuchas ilegales a magistrados, políticos y periodistas en Colombia, la CIDH y su Relator Especial para la Libertad de Expresión, Edison Lanza, manifestaron que "*el uso de cualquier programa o sistema de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación, y contar con control judicial previo. La vigilancia de las comunicaciones y las injerencias a la privacidad que excedan lo estipulado en la ley, que se orienten a finalidades distintas a las autorizadas por ésta o las que se realicen de manera clandestina deben ser drásticamente sancionada*s". En otro comunicado en igual sentido, reiteraron qu*e "la CIDH ha establecido que la vigilancia masiva de comunicaciones en ningún caso podrá ser considerada como proporcional. En la misma*

línea, la recolección sistematizada de datos públicos –voluntariamente expuestos por el propietario de dichos datos, como publicaciones en blogs redes sociales, o cualquier otra intervención de dominio público- también constituye una injerencia en la vida privada de las personas. El hecho de que la persona deje rastros públicos de sus actividades –en internet de manera inevitable- no habilita al Estado a recolectarla sistemáticamente salvo en las circunstancias específicas donde dicha injerencia estuviera justificada".

En la normativa Argentina, la inteligencia está permitida bajo autorizaciones y límites específicos, de conformidad con las disposiciones de la Ley de Inteligencia Nacional 25.520, Decreto 1311/15 y ss., la Ley de Seguridad Interior y el Código Procesal Penal de la Nación. La Ley 25.520 entiende por Inteligencia Nacional a "*la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación*" (2) , y por inteligencia criminal a *"la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional*" (3), y establece que *«ningún organismo de inteligencia podrá: 1. Realizar tareas represivas, poseer facultades compulsivas, ni cumplir funciones policiales o de investigación criminal»*. (4).

La Ley de Inteligencia 25.520 no prohíbe expresamente la posibilidad de que la inteligencia se realice sobre fuentes de acceso público. De hecho, el Decreto 1311/15 que aprueba la "Nueva Doctrina de inteligencia Nacional", define a la información de inteligencia como "a*quella que comprende las observaciones y mediciones* ***obtenidas o reunidas de fuentes públicas*** *o reservadas, referidas a eventos o problemáticas relevantes del ámbito de la defensa nacional o de la seguridad interior, o que tienen incidencia en estas esferas, y cuya recolección, sistematización y análisis permite elaborar un cuadro de situación del conjunto de las problemáticas en el nivel estratégico o en el nivel táctico*" (el subrayado es propio).

Sin perjuicio de la norma en materia de inteligencia y las definiciones que la propia ley nos trae, el Protocolo de Ciberpatrullaje resalta que las tareas de prevención policial del delito en fuentes digitales abiertas no son tareas de inteligencia criminal, sino tareas inherentes a las funciones de las fuerzas de seguridad. Aquí es donde comienza la confusión: ¿cuál es la diferencia entre tareas de inteligencia y tareas de prevención del delito (entendidas como vigilancia)?

La diferencia entre vigilancia e inteligencia es confusa y, desafortunadamente, el marco jurídico argentino no aporta claridad suficiente. Si bien puede argumentarse que la vigilancia o patrullaje pareciera ser una facultad inherente a los deberes de las fuerzas policiales y de seguridad, las actividades de inteligencia, como lo mencionamos al principio, requieren autorizaciones específicas y poseen límites para su aplicación con relación a crímenes específicos, de conformidad con las disposiciones de la Ley de Inteligencia Nacional 25.520.

Carolina Botero, Directora de la Fundación Karisma de Colombia, destaca en este artículo que si bien OSINT "*es una actividad legítima y útil para cualquiera*", el inconveniente está en cuándo su uso deja de ser monitoreo y pasa a ser vigilancia o acoso o acecho de una persona. Sobre ello, concluye que cuanto más individualizado sea el monitoreo de fuentes abiertas, más se aleja del monitoreo y más se convierte en vigilancia, siendo ésta una *"actividad regulada, que exige controles y no puede hacerse por motivos de raza, religión o preferencias políticas"*. Dicho ello, pareciera identificar a la anonimización o despersonalización de la información como uno de los elementos distintivos entre las distintas prácticas. Este es un punto relevante en la discusión ya que hay quienes consideran que, por el contrario, el monitoreo indiscriminado puede enmarcarse dentro de tareas de inteligencia.

En el ámbito nacional, tanto la Fundación Vía Libre como el CELS consideran que las actividades contempladas en el Protocolo exceden «el patrullaje» y constituyen efectivamente inteligencia.

Sobre los delitos que se monitorean:

Por otra parte, el Protocolo establece una alarmante cantidad de delitos objeto de las tareas de prevención (que, dicho sea de paso, algunos de ellos no parecen tener relación directa con la emergencia sanitaria ocasionada por la pandemia). Se propicia un monitoreo amplio, que además de ir en contra de los principios de protección de datos personales establecidos en la Ley 25.326, choca con los requisitos de especificidad mencionados en la normativa de inteligencia nacional. Cualquier recolección indiscriminada de información con el fin de, a posteriori, analizar si constituye o no un ilícito, va en contra de la naturaleza de dicha norma. Al respecto, el CELS sostuvo que "*se requiere de un mínimo grado de sospecha sustantiva respecto de la existencia de determinado fenómeno criminal (de ahí la expresión «específica»), con cierta delimitación*

espacial, temporal y/o personal, y en relación a la probabilidad de encontrar datos relevantes en la fuente abierta de que se trate". Las actividades de inteligencia no pueden ser utilizadas como un cheque en blanco al reunir información a través de fuentes públicas, para luego analizarla a fondo y descartar cualquier actividad delictiva.

Consecuencias en la libertad de expresión:

Son varios los estudios que demuestran el impacto "silenciador" que las prácticas de OSINT y SOCMINT tienen sobre el discurso: las personas tienden a callarse si saben que están siendo vigiladas, especialmente al publicar contenido en redes sociales. En palabras de Karen Gullo, analista de la Electronic Frontier Foundation, *"Lo que sucede es que las personas empiezan a auto-vigilar sus comunicaciones: es más probable que eviten asociarse con ciertos grupos o individuos, o mirar sitios web o artículos, cuando creen que el gobierno los está vigilando a ellos o a los grupos o personas con los que se conectan. Esto perjudica a nuestra democracia y a la sociedad en su conjunto*" (la traducción es propia).

Desde el CELE analizamos el Protocolo desde una mirada crítica con relación al impacto que este tipo de procedimientos puede tener en los derechos humanos, fundamentalmente en el derecho a la libertad de expresión. Nos preocupa la falta de normativa clara para encuadrar este tipo de actividades al interior del Ministerio de Seguridad y la falta de claridad en torno a la supervisión de estas tareas. Preocupa, a su vez, la falta de transparencia en cuanto a los sistemas utilizados, los medios para llevar adelante estas tareas y la seguridad de los datos recabados. Finalmente, preocupa también la falta de proporcionalidad con la que las fuerzas de seguridad están actuando en la investigación y detención de algunas personas a raíz de lo que comentan en redes sociales, y el uso forzado de tipos penales como el de amenazas (artículo 149 bis CPN) o de intimidación pública (artículo 211 CPN), que no fueron pensados a estos efectos. Basta con conocer los casos de Kevin Guerra y los allanamientos *"contra agitadores en las redes"*. Estos son algunos de los casos que conocemos ya que se volvieron "famosos", pero desconocemos cuántos más existen, judicializados, que hayan pasado desapercibidos.

A fin de saldar algunas de estas cuestiones que desconocemos, a principios de septiembre realizamos un pedido de acceso a la información pública ante el Ministerio de Seguridad a fin de que se respondan, entre otras, las siguientes preguntas (5):

- ¿Se ha suspendido la aplicación del Protocolo a raíz de la Nota de la Agencia de Acceso a la Información Pública?
- Sobre el total de las tareas de prevención policial del delito en el espacio cibernético, ¿qué porcentaje se realiza de forma automatizada, sin intervención de agentes de seguridad revisando el contenido visualizado?
- ¿Cuántos casos surgidos de las tareas de prevención policial del delito en el espacio cibernético se judicializaron? Indique cuántos delitos se encontraron mediante el monitoreo, correspondiente a cada uno de los delitos mencionados en el artículo 3º del Protocolo, desde la entrada en vigencia del mismo.
- ¿Qué medidas de seguridad se implementan sobre las bases de datos que albergan la información obtenida a raíz de las tareas de prevención policial del delito en el espacio cibernético?

El pasado 25 de septiembre se llevó a cabo la reunión bimensual de la Mesa Consultiva que tiene como finalidad evaluar la observancia del Protocolo, de conformidad con el Artículo 3º de la Resolución 144/20 del mencionado organismo. El encuentro contó con la participación de representantes de organizaciones de la Sociedad Civil, entre ellos Beatríz Busaniche de la Fundación Vía Libre, quien compartió en su "*Resumen semanal de Noticias y novedades"* los puntos más relevantes de la reunión. Al menos una de las preguntas que formulamos en nuestro pedido de información fue contestada en la reunión: las autoridades confirmaron que no adquirieron ningún dispositivo o sistema para la realización de las tareas de prevención a las que alude el Protocolo.

Sin embargo, las respuestas del Ministerio dejan serias incógnitas abiertas. Entre los puntos a destacar, es alarmante que las tareas de prevención se realicen "a mano", según lo indicado por las autoridades en la reunión. ¿Qué significa esto? ¿Cómo se llevan a cabo estas tareas en el día a día? Cómo anonimizar el contenido siendo el monitoreo «manual»?

El impacto de la inteligencia en redes sociales en nuestros derechos fundamentales cobra mayor relevancia en la situación actual de pandemia donde, cada vez más, nuestras vidas se desarrollan a través de un dispositivo electrónico. Como sociedad, tenemos que exigir las rendiciones de cuentas correspondientes y alzar la voz –como lo han hecho numerosas organizaciones– para alertar sobre los peligros de estas prácticas y asegurar que se respeten nuestros derechos humanos. **Esperamos que, en respuesta a nuestro pedido de acceso a**

la información, el Ministerio aclare las inquietudes que nos preocupan.

Notas al pie:

1. “Seguidores que no vemos. Una primera aproximación al uso estatal del Open-source Intelligence (OSINT) y Social media intelligence (SOCMINT)”, Asociación por los Derechos Civiles (ADC), 2018, disponible para descargar aquí.
2. Artículo 2.1 de la Ley 25.520
3. Artículo 2.3 de la Ley 25.520
4. Artículo 4 de la Ley 25.520
5. La solicitud de acceso fue ingresada el día 8 de septiembre del 2020 y a la fecha de esta publicación, aún no hemos obtenido respuesta. Haga click aquí para descargar la solicitud de información completa.

Por Morena Schatzky (@morschatzky) y Agustina Del Campo (@agustinadelcamp)

PhotoCredit: @matthewhenry

-