Buenos Aires, 21 de abril del 2020

Ref: Respuesta al borrador "Reglamento general para la realización de tareas de ciberpatrullaje por parte de las fuerzas de seguridad dependientes del Ministerio de Seguridad de la Nación federales bajo la jurisdicción de las autoridades responsables para su ejercicio".

A la Sra. Ministra de Seguridad de la Nación

Lic. Sabina Andrea Frederic

Por la presente, desde Fundación Vía Libre y el Instituto Latinoamericano de Seguridad y Democracia (ILSED), venimos a dar respuesta al borrador de la Resolución ministerial que establece el *"Reglamento general para la realización de tareas de ciberpatrullaje por parte de las fuerzas de seguridad dependientes del Ministerio de Seguridad de la Nación federales bajo la jurisdicción de las autoridades responsables para su ejercicio"* (en adelante, "Reglamento"), que nos fuera remitido el pasado 17 de abril luego de la reunión e intercambio de opiniones entre funcionarios de ese Ministerio y diversas organizaciones de la sociedad civil.

Tras haber realizado un análisis pormenorizado del proyecto recibido, consideramos necesario subrayar las graves vulneraciones a los derechos humanos, como el derecho a la privacidad y a la libertad de expresión, que puede provocar la práctica referida en los términos en que se pretende regular, recomendando por lo tanto la suspensión de estas actividades.

Lo que el Reglamento denomina "ciberpatrullaje", concepto que carece de significado técnico o jurídico, y tal como está definido en los arts. 2 a 5, es en realidad una práctica de inteligencia, cuyo alcance corresponde a la disciplina de recolección denominada

"inteligencia de fuentes abiertas" (OSINT)[1] y más particularmente "inteligencia de medios sociales" (SOCMINT)[2].

La actividad referida debe ser entendida como inteligencia, en este caso, inteligencia criminal, porque supone un proceso de recolección y análisis de información que concluye con una evaluación de si existe o no una amenaza a la seguridad interior. Se distingue de otros tipos de prácticas policiales dirigidas a la prevención, como el patrullaje callejero, entre otras cosas, porque se realiza de manera anónima o encubierta y, por lo tanto, no se advierte a las personas que están siendo vigiladas.

El Ministerio de Seguridad de la Nación y las diversas fuerzas están autorizados a realizar tareas de inteligencia criminal, conforme lo establecen la ley de inteligencia y la ley de seguridad interior, pero bajo el resguardo de ciertos límites[3]. El primero vinculado con su método o forma de realización y el segundo vinculado con su objetivo o finalidad. Sin embargo, el Reglamento no precisa cuáles son los métodos de vigilancia a ser utilizados ni cómo se hace para discernir una mera opinión de una eventual práctica criminal. En nuestra reunión hemos consultado sobre estos puntos fundamentales, porque de ello depende su licitud, pero aún no hemos obtenido respuesta. La vigilancia masiva indiscriminada no se encuentra regulada en nuestro país y, más grave aún, la inteligencia sobre opiniones y actividades lícitas, entre otras finalidades, está terminantemente prohibida (art. 4 de la ley 25.520).

Realizar una vigilancia del modo en el cual lo plantea el Reglamento es muy peligroso para los derechos y garantías que fundan nuestra democracia. Los sistemas informáticos que recogen palabras o frases no tienen capacidad de identificar la razón o motivación por

---

[1] Véase: *inter alia*: Steele, R. D. 1997. "Open Source Intelligence: What Is It? Why Is It Important to the Military?". *READER Proceedings*, Vol 2., pp. 329-341; Richelson, J. 2015. *The U. S. Intelligence Community*. New York: Routledge; Lowenthal, M. M.. 2006. "Open-Source Intelligence: New Myths, New Realities" en George, R.Z. et al. I*ntelligence and the national security strategist: enduring issues and challenges*, p. 273-278, Lanham, Md. Rowman & Littlefield. Compárese también con la legislación de los Estados Unidos: National Defense Authorization Act of 2006, Pub. L. 109-163, §931, 119 STAT. 3411.

[2] Omand, D., Bartlett J. & Mille C.r 2012. "Introducing Social Media Intelligence (SOCMINT)". *Intelligence and National Security*, 27(6):801-823.

[3] Concretamente en el encuadramiento legal vigente, las actividades de inteligencia que el Reglamento procura regular corresponden a la definición de inteligencia criminal (Ley 25520, art. 2º, inc. 3) y su ejecución corresponde, conforme al mismo marco legal (id., art. 9º) a la Dirección Nacional de Inteligencia Criminal.

las que han sido utilizadas, y la participación humana que intentara corregir esto solo podría hacerlo después de la captación de miles de comunicaciones irrelevantes. Que, incluso, podrían aparejar la apertura de causas penales en contra de sus autores/as o difusores/as, como se ha demostrado empíricamente en el transcurso de los últimos días (y los últimos años).

En este sentido, el Reglamento define la información a reunir, procesar y analizar como aquella "de carácter público" (art. 2º). Ahora bien, el hecho de que determinados datos estén disponibles en fuentes normalmente accesibles al público en general[4] no implica necesariamente que no se trate de intromisiones en el ámbito de las acciones privadas, protegido por el art. 19 del texto constitucional. Así como en una conversación llevada a cabo en el espacio físico público, los interlocutores pueden esperar razonablemente la ausencia de intromisiones sistemáticas de terceros -aunque no estén libres de observación fortuita- existe una cierta expectativa de privacidad en estos ámbitos digitales, con el agravante de que, en estos últimos, las intromisiones se producen de manera subrepticia, no detectable normalmente por las personas afectadas[5].

Estas intromisiones en la vida privada, particularmente en los casos de explotación de actividades generalizadas e inespecíficas de vigilancia, producen en el público un efecto intimidatorio (*chilling effect*)[6] que afecta directa y gravosamente el derecho a la libertad de opinión y expresión afirmado en la interpretación constitucional y en los tratados de derechos humanos. En la práctica, el conocimiento de la existencia de estas formas de vigilancia indiscriminada y la ambigüedad induce en el público conductas de autocensura

[4] En sentido estricto, las redes sociales y otras fuentes de información disponibles a través de la Internet no son públicas, por cuanto el derecho de exclusión corresponde a personas jurídicas de derecho privado y no se hallan en el dominio público. En términos generales, se encuentran protegidas por las regulaciones de derecho de autor y otras regulaciones de propiedad intelectual o industrial.

[5] Así ha sido reconocido en la jurisprudencia comparada de derechos humanos. Por ejemplo, en Peck v. Reino Unido, la Corte Europea de Derechos Humanos ha hecho notar que "existe [...] una zona de interacción de una persona con otras, aún en un contexto público, que puede estar comprendida dentro de los alcances de 'vida privada'". Corte Europea de Derechos Humanos (Cuarta Sección). 2003. Case of Peck v. The United Kingdom. Application No. 44647/98. Fallo de 28 de enero de 2003 (versión final de 28 de abril 2003). Véase también, en el mismo sentido y del mismo tribunal (Quinta Sección), 2010, Case of Uzun v. Germany. Application No. 35623/05. Fallo del 2 de septiembre 2010 (versión final de 2 de diciembre 2010).

[6] En el Derecho comparado, véase entre otros Suprema Corte de los Estados Unidos, voto del *justice* Black en *Wieman v. Updegraff*, 344 U.S. 183 (1952) a 196; Corte Superior de Justicia de Ontario, *Iorfida v. MacIntyre*, 1994 CanLII 7341 (ON SC).

desalentando el ejercicio de derechos legítimos. Al mismo tiempo se produce otro efecto contraproducente en la esfera pública, como ser que manifestaciones que de otro modo no hubieran adquirido notoriedad por irrelevantes o falsas, o expresadas como sarcasmos o ironías, o que no representan amenaza de violencia concreta e inminente, adquieren relevancia pública. Esto es conocido como "efecto Streisand".[7] Así, lo que de otro modo hubiera resultado intrascendente causa un efecto de repercusión y conmoción pública innecesario.

En este contexto, cabe destacar que las acciones de inteligencia de fuentes abiertas pueden estar dirigidas: a blancos específicos (*target-oriented intelligence*), esto es, personas identificadas o identificables sobre las que existe razonable sospecha de que se encuentran vinculadas a la preparación o la comisión de ilícitos indeterminados (por ejemplo, actividades ligadas al crimen organizado o apuntadas contra el orden constitucional); a acciones específicas (*event-oriented intelligence*), como la obtención de información que permita identificar o localizar a los partícipes en un delito determinado o sus actos preparatorios; y, a actividades generalizadas de vigilancia que implican la búsqueda extensiva y sistemática de potenciales ilícitos sin requerimiento específico previo de blancos o acciones sujetas a escrutinio (lo que en la jerga informal de las prácticas de inteligencia se conoce como *to go fishing o* "salir de pesca").

En un estado democrático de derecho, cada una de ellas requiere de salvaguardas bien establecidas para evitar la violación de garantías fundamentales y, en la medida que la esfera afectada sea mayor, deben ser más restrictivas. Como criterio general, la última forma mencionada solo se justifica en presencia del debido marco legal y en circunstancias muy excepcionales, cuando no es posible contrarrestar una amenaza por ningún otro medio menos lesivo.

[7] Se denomina de esta forma, por la actriz estadounidense Barbra Streisand, quien en 2003 demandó el retiro de exhibición pública de una fotografía aérea —identificada como "imagen 3850", parte de un proyecto destinado a mostrar la erosión de zonas costeras de California— en la que aparecía su mansión en Malibu. Al momento de presentarse la demanda, la imagen había sido descargada del sitio del autor solo seis veces (dos de ellas, por los abogados de Streisand); en el mes siguiente a la presentación fue descargada más de 420000 veces. La demanda fue rechazada con costas a la actora (California Superior Court, Streisand v. Adelman, et al., Case SC077257).

Es por ello que consideramos que, conforme a todas estas fundamentaciones los principios y prohibiciones planteados en el Reglamento entran en serias contradicciones con lo que establece en su desarrollo. Entre los puntos del Reglamento que entendemos más problemáticos y que refuerzan el rechazo a la iniciativa, cabe mencionar:

- En ninguna parte del Reglamento, ni en otro documento público del que tengamos conocimiento, se ha establecido el principio de necesidad para la utilización del "ciberpatrullaje". No parece haber evidencia empírica, ni siquiera parcial, de que las actividades de reunión, procesamiento y análisis de información sistemáticas, generalizadas e indiscriminadas, que el Reglamento permite, tengan efectos positivos en la prevención de delitos.

- El Reglamento es tan amplio y vago en sus finalidades y definiciones, que impide que cumpla una función real de delimitar la práctica policial. La pretensión simultánea de establecer un método de prevención, de identificación de alertas tempranas, de detección de delitos en flagrancia y de regular una "investigación preliminar" confunde los planos y dificulta la efectiva protección de los derechos y garantías constitucionales que el Reglamento declara respetar.

- El Reglamento no establece un marco referencial de requerimientos de inteligencia, y tampoco indica a quienes les corresponde generar dichos requerimientos. En consecuencia, no surge cuáles serían los delitos que quedarían comprendidos bajo su alcance. Se establece allí que el "ciberpatrullaje" será utilizado "para la prevención y detección de delitos que requieran de la utilización de sistemas informáticos como medio comisivo accesorio o principal para su desarrollo". La definición propuesta podría alcanzar a la mayoría de los delitos del Código Penal de la Nación, lo que en buena medida vuelve abstracta la evaluación sobre los principios de necesidad y proporcionalidad. Con esa regulación, se deja un margen de actuación demasiado amplio tanto a las autoridades políticas como a las fuerzas de seguridad.

- Como consecuencia de la omisión en establecer los fundamentos del principio de necesidad, y de la ausencia de un marco referencial para los requerimientos de

inteligencia, no se establecen criterios para limitar al mínimo necesario las intervenciones proporcionándole marcos de actuación restringidos y concretos, lo que implica permitir vigilancia masiva e indiscriminada sobre la ciudadanía.

- El Reglamento no proporciona un marco normativo concreto a las actividades que procura regular. Es notoria la ausencia de normas sobre la minimización de información, esto es, la eliminación inmediata e irreversible de todo registro que no esté relacionado con el requerimiento de inteligencia específico, y las salvaguardas para garantizar dicha eliminación.

- El Reglamento no hace referencia a cómo se realizará la compartimentación de las actividades de reunión, procesamiento, análisis y difusión; a los lineamientos de los métodos y las técnicas a aplicar en cada fase del ciclo; ni las directrices sobre adquisición, utilización y disposición de los elementos tecnológicos a emplear en la ejecución de cada una de las actividades.

- Existe una tendencia marcada en el Reglamento a emparentar el "ciberpatrullaje" con el patrullaje en la vía pública, cuando son actividades que revisten distintas características y condiciones de legalidad. Una de ellas, por ejemplo, es que en el espacio público siempre existe algún tipo de escrutinio sobre la vigilancia. Por eso es que, para la prevención, a los miembros de las policías y fuerzas de seguridad se les exige la utilización de identificaciones y uniformes. Para reforzar esta idea, como hemos mencionado, nótese que en la vía pública no es tolerable que la policía se acerque a escuchar y registrar las conversaciones entre las personas reunidas en una plaza, o que se infiltre en manifestaciones o asambleas. Una actividad de inteligencia, en cambio, no es observable, ni a su respecto pueden cumplirse estos requerimientos.

- No quedan claras las responsabilidades de los diversos organismos vinculados con las actividades que se pretende regular. Se genera, así, una probabilidad muy elevada de que las fuerzas policiales y de seguridad incurran en arbitrariedad. No se establecen criterios ni responsabilidades de control, auditoría y transparencia que

permitan garantizar que las acciones planeadas se llevan a cabo con pleno respeto de las garantías fundamentales.

Sumado a estos ejes, al observar los resultados de la realización de actividades de inteligencia de fuente abierta por parte de las fuerzas de seguridad federales hasta la fecha, se puede concluir que se trata de una práctica que evidentemente genera un gran impacto social y es de dudosa eficacia para la prevención y la detección de hechos criminales. También debe tomarse en cuenta el efecto imitativo que generan estas prácticas en las policías provinciales, muchas de las cuales ya cuentan con divisiones de ciberdelitos, lo que podría ampliar aún más la arbitrariedad y falta de control.

Consideramos que, en los términos planteados, el Reglamento se encuentra notoriamente por fuera de los márgenes de legalidad y constitucionalidad y su uso actual implica someter a un riesgo innecesario los derechos de la ciudadanía, con una probabilidad muy elevada de que se instalen prácticas difíciles de erradicar, como ha ocurrido en los ámbitos de seguridad e inteligencia en nuestro país a lo largo del tiempo.

Por todas estas razones, sin dejar de entender la necesidad y urgencia que tiene el Ministerio de Seguridad de la Nación de garantizar la protección de las todas las personas en un contexto excepcional como es la actual emergencia sanitaria, recomendamos enfáticamente que se deje sin efecto la propuesta de Reglamento, se derogue la normativa vigente y se reemplace por una normativa acotada a determinados delitos de gravedad, con las consideraciones aportadas en este documento, hasta tanto sea posible la discusión democrática que exige la Constitución Nacional en el seno del Congreso de la Nación.

Quedamos a su disposición para realizar los aportes que sean necesarios y consideren pertinentes. La saludan cordialmente,

Fundación Vía Libre **Instituto Latinoamericano de Seguridad y Democracia**

Fundación
Vía Libre

ilsed
Instituto latinoamericano de seguridad y democracia