AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Buenos Aires, 21 de abril de 2020

A: Dra. Sabina Andrea Frederic
Ministra de Seguridad de la Nación

S / D

C/C: Lic. Valentina Novick
Subsecretaria de Investigación Criminal y Cooperación Judicial
Secretaría de Seguridad y Política Criminal
Ministerio de Seguridad de la Nación

S / D

De nuestra mayor consideración,

Desde Amnistía Internacional, agradecemos la invitación enviada por este Ministerio de Seguridad de la Nación el pasado el 17 de abril de 2020 para participar del proceso de consulta con relación al proyecto de resolución por la que este Ministerio crea 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".

Como hemos expresado en distintas oportunidades, Amnistía Internacional valora el enorme esfuerzo que está llevando adelante el gobierno nacional para controlar la expansión del COVID19. El gobierno tiene la obligación de garantizar el derecho a la salud y de prevenir, tratar y controlar la pandemia. Con este fin, puede restringir temporalmente algunos derechos humanos para responder a situaciones puntuales y coordinadas. Sin embargo, Amnistía Internacional advierte que, en este marco de excepcionalidad y conforme lo establece el derecho internacional, es esencial que las medidas que se adopten respeten el ejercicio de los derechos humanos y las garantías constitucionales vigentes.

En este sentido, el llamado "ciberpatrullaje" -o investigación en fuentes abiertas de datos- es una actividad de inteligencia que puede poner en entredicho derechos fundamentales como la libertad de expresión y la privacidad; a la vez que puede debilitar el funcionamiento del sistema democrático al producir un efecto silenciador sobre voces disidentes.

Por esta razón, las consideraciones presentadas en este documento buscan contribuir a que el marco regulatorio aplicable a la implementación de tareas de inteligencia de esta naturaleza tenga como premisa el respeto y garantía de los derechos humanos, incluyendo – entre otros aspectos – la debida necesidad y proporcionalidad acordes a un fin legítimo, una adecuada rendición de cuentas frente a las tareas llevadas a cabo y la previsión de las responsabilidades oportunas en caso de incumplimiento de los límites preestablecidos.

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Esperando que lo aportes presentados a continuación contribuyan efectivamente a la elaboración del proyecto de resolución en cuestión, seguimos a disposición para participar de futuras instancias de diálogo sobre esta agenda, así como para ampliar esta u otra información.

Sin otro particular, la saluda cordialmente.

Mariela Belski
Directora Ejecutiva
Amnistía Internacional Argentina

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Consideraciones respecto del proyecto normativo de Resolución del Ministerio de Seguridad de la Nación por la que se aprueba 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"

I. Ciberpatrullaje y tareas de vigilancia en el marco del control de la pandemia y el respeto a los derechos humanos

El Proyecto de reglamento bajo análisis busca regular el ejercicio por parte de las fuerzas de seguridad de actividades de vigilancia en fuentes abiertas de datos, conocidas como *"open source intelligence"* (OSINT) o *"social media intelligence"* (SOCMINT). En otras palabras, como se encuentra definido en el art. 2 del Proyecto de Reglamento en análisis, *"el ciberpatrullaje consiste en el monitoreo, observación, análisis de la información de carácter público presente en fuentes digitales abiertas, redes sociales y plataformas de comunicación e información digital, con el objetivo de identificar eventos que afecten o puedan afectar la situación de seguridad interior"*.

El uso de las técnicas de investigación en fuentes abiertas por parte de los organismos estatales, particularmente para tareas de seguridad pública, puede tener una serie de implicaciones para la garantía de los derechos humanos, como la privacidad, la libertad de expresión, reunión y asociación, entre otros.

Amnistía Internacional entiende que la pandemia de COVID-19 es una emergencia global de salud pública, que precisa de una respuesta coordinada y a gran escala de los gobiernos en todo el mundo. La tecnología puede y debe desempeñar importantes funciones durante este esfuerzo que se está realizando para salvar vidas y preservar la seguridad ciudadana. Sin embargo, se corre el riesgo que las iniciativas para contener el virus terminen expandiendo los sistemas de vigilancia digital invasiva.

En tiempos extraordinarios, el derecho de los derechos humanos sigue siendo aplicable. De hecho, el marco de los derechos humanos tiene por objeto garantizar un cuidadoso equilibrio de los distintos derechos para proteger a las personas y las sociedades en general. Los Estados no pueden comprometer la privacidad y la libertad de expresión con el pretexto de gestionar una crisis de salud pública.

Por esto, Amnistía Internacional viene monitoreando en distintos países el empleo de tecnologías de vigilancia en el marco del contexto actual de emergencia de salud global[1]. En cada caso, busca garantizar que los gobiernos no usen tecnologías de vigilancia para recopilar formas de datos más allá de los que sean legítimamente necesarios para contener la enfermedad. Además, los gobiernos deben abordar los motivos de preocupación relacionados con la protección de datos y la discriminación.

De esta forma, las medidas adoptadas en este contexto de emergencia sanitaria por el gobierno argentino, deben tener una duración limitada y prolongarse sólo durante el tiempo necesario para abordar la pandemia actual. También deben ser transparentes y claras, para que puedan ser analizadas y modificadas, retiradas o anuladas posteriormente, si procede. Bajo ningún concepto, la pandemia

[1] Para más información, consultar "COVID-19: Vigilancia y amenaza para tus derechos": https://www.amnesty.org/es/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/ (úúltimo acceso en 19 de abril de 2020) .

AMNISTÍA INTERNACIONAL

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

de COVID-19 debe servir de excusa para que el gobierno adopte medidas de vigilancia masiva indiscriminada.

El gobierno también debe garantizar que los datos recopilados, conservados y agregados para responder al contexto de emergencia sanitaria tengan un alcance y duración limitados en función de la pandemia y no utilizarse con fines comerciales ni de otra índole. Asimismo, debe hacer todo lo posible para proteger los datos personales, lo que incluye garantizar la debida seguridad de los datos recopilados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, tratamiento y almacenamiento.

El aumento de las medidas de vigilancia ante la COVID-19 también tiene que estar sujeto a la supervisión efectiva de organismos independientes de control externo y control judicial. Además, se debe ofrecer a las personas la oportunidad de conocer e impugnar toda medida que se tome en relación con la COVID-19 para recopilar, agregar, conservar y emplear datos. Las personas que hayan sido sometidas a vigilancia deben tener acceso a medios efectivos para interponer recursos.

Finalmente, las respuestas a la COVID-19 que contengan medidas de recopilación de datos deben incluir medios de participación libre, activa y significativa de las partes interesadas pertinentes, razón por la que Amnistía Internacional valora esta instancia de participación y espera que esta práctica se sostenga con relación a la implementación de las medidas de ciberpatrullaje en cuestión y a las demás tareas de vigilancia que puedan afectar los derechos humanos de la población.

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

II. Comentarios al Proyecto de Resolución y Reglamento

II.a. Consideraciones generales

En lo que sigue Amnistía Internacional acercará una serie de consideraciones sobre el proyecto de resolución por la que el Ministerio de Seguridad de la Nación crea 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"*. Las observaciones abordarán, en primer lugar, el texto propuesto en el Reglamento, Anexo que acompaña a la Resolución; y luego marcaremos algunos aspectos adicionales que entendemos necesarios sean tenidos en cuenta para su incorporación.

Por lo demás, Amnistía Internacional remarca una preocupación general acerca del texto del Reglamento presentado. Como normativa que busca incrementar los poderes de vigilancia en un contexto de Estado de emergencia sanitaria, los principios, criterios y directrices en ella previstos deben ser establecidos con el mayor grado de precisión posible, de modo de evitar que éstos queden supeditados a la discrecionalidad de funcionarios públicos o miembros de fuerzas de seguridad. En este sentido, encontrarán algunos comentarios sobre disposiciones ambiguas que debería ser detenidamente revisadas.

II.b. Comentarios al Proyecto de Reglamento

1. La excepcionalidad de la medida

Artículo 1. El presente documento tiene por finalidad establecer principios, criterios y directrices generales para la realización de las tareas de ciberpatrullaje por parte de los cuerpos policiales y fuerzas federales de seguridad durante el tiempo de vigencia del Decreto de Necesidad y Urgencia DECNU 260-2020 del 12 de marzo de 2020.

Comentario:

Uno de los rasgos que hemos explicitado previamente es la excepcionalidad del ciberpatrullaje como medida para coadyuvar a la situación pandémica que nos aqueja. Una manifestación de esa excepcionalidad es la temporalidad de las medidas, es decir, que la vigencia temporal del ciberpatrullaje se encuentre directamente vinculada con la extensión de la situación que le dio origen.

En este sentido, el artículo 1 del Anexo prescribe que el reglamento tendrá la vigencia conforme lo dispuesto por el DNU 260-2020. Dicho decreto, a su vez, establece la ampliación de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, en virtud de la Pandemia por el plazo de un (1) año a partir de la entrada en vigencia del mismo -12 de marzo de 2020-.

Nuestra primera observación es la falta de claridad respecto a qué sucederá una vez cumplido ese plazo, puesto que es la vigencia de la Resolución la que se pierde ante el cumplimiento del mismo, pero nada dice sobre la continuidad -o no- de la realización de tareas de ciberpatrullaje. Esto podría acarrear que el Estado continúe realizando tareas de esa naturaleza sin el marco regulatorio aquí propuesto.

Tampoco surge con claridad si el ciberpatrullaje es entendido como una práctica excepcional y sólo vinculada a la situación actual, o en realidad formará parte de las políticas públicas en materia de seguridad de la actual administración.

Por último, ni la Resolución ni el anexo disponen qué tipo de vinculación normativa tienen con la Resolución 2018-31-APN-SECSEG que dispuso una serie de instrucciones al área de ciberdelito del Ministerio de Seguridad. Durante la vigencia de la presente regulación, ¿mantiene su

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

validez la segunda?, ante el cumplimiento del plazo antes remarcado ¿el ciberpatrullaje dejará de practicarse o continuará bajo la regulación de la Resolución 2018-31? Son todos interrogantes que no están claros en la Resolución bajo análisis.

Recomendación:
En función de estas lagunas interpretativas, sugerimos que se aclare expresamente en la normativa que el ciberpatrullaje es una práctica excepcional vigente durante el período de la pandemia. En caso de que se pretenda sostener algún grado de tareas de ciberpatrullaje luego de la situación pandémica, sería necesario que antes del cumplimiento del plazo de la presente Resolución, se proponga otra instancia para el diseño de un nuevo marco normativo para dichas actividades, que, por fuera de la excepcionalidad que atraviesa la situación actual, pueda ser debatido en profundidad por el Congreso de la Nación.

2. La vigilancia masiva y las hipótesis delictivas
Artículo 4º. El ciberpatrullaje es una actividad de los cuerpos policiales y fuerzas federales de seguridad con el objetivo de identificar, prevenir y alertar sobre la posible ocurrencia de delitos de acción pública, como así también para investigar, de manera preliminar, actividades que podrían revestir carácter ilícito, a fin de simultáneamente realizar las comunicaciones que correspondan a las autoridades jurisdiccionales competentes.
Artículo 5º. Las policías y fuerzas de seguridad federales realizan tareas de ciberpatrullaje con el objetivo de: a. identificar posibles delitos; b. establecer alertas tempranas dirigidas a prevenir la ocurrencia de posibles hechos criminales y/o eventos delictivos; c. investigar, de forma preliminar, posibles hechos delictivos para su posterior comunicación a las autoridades jurisdiccionales que correspondan.

Comentario:
Como puede observarse, ambos artículos permiten que las fuerzas de seguridad implementen actividades de ciberpatrullaje para detectar delitos en general. Es decir, habilitan un sistema de control de toda la actividad en las redes sociales, basado en búsquedas aleatorias de frases o palabras claves para detectar la comisión de delitos. De allí que las fuerzas de seguridad quedan habilitadas para realizar tareas de vigilancia masiva sin que exista una hipótesis delictiva previa. Sin embargo, y conforme lo establece la Ley de Inteligencia -Ley 25.520, artículo 4-, sólo se encuentran permitidas las tareas de inteligencia criminal y de investigación policial siempre que éstas estén destinadas a intervenir sobre amenazas delictivas concretas.

A ello se le debe añadir la advertencia adicional sobre los riesgos de que eventualmente se llegaran a adoptar algoritmos para la identificación de expresiones o frases, ya que este tipo de tecnología no tiene la capacidad de reconstruir el contexto en el que éstas se realizan lo que torna sumamente peligrosa esta práctica -sobre esta cuestión ver el punto 3 del presente-.

Propuesta:
Circunscribir expresamente la actuación de las fuerzas de seguridad a los supuestos en que existan hipótesis criminales concretas; prever los supuestos a los que se le puede aplicar, desagregar expresamente la prohibición de actuar sin los mismos.

3. El ciberpatrullaje y la Libertad de expresión

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Artículo 6º – Los cuerpos policiales y fuerzas de seguridad federales realizarán las tareas de ciberpatrullaje cumpliendo estrictamente los siguientes principios de actuación: (…) c. Derechos a la libertad de expresión. Las tareas de ciberpatrullaje no implicarán en modo alguno la afectación al derecho a la libertad de expresión garantizado por la Constitución Nacional y los Tratados Internacionales de Derechos Humanos de los que el Estado Argentino es signatario, así también como de toda la normativa legal específica que los garantice.

Comentario:

Considerando el hecho de que ninguna tarea de vigilancia debe violar nuestros compromisos constitucionales fundamentales tales como la libertad de expresión, este reglamento debería garantizar en sus disposiciones un marco claro, estricto, y transparente de actuación que, en sí mismo, vele por que la implementación de las actividades de ciberpatrullaje en la práctica no afecte los derechos humanos.

A este respecto, vale recordar que el ciberpatrullaje representa riesgos de condicionamiento del discurso público produciendo el llamado *chilling effect*: si una persona sabe -o tiene la sospecha fundada- que todo lo que comenta, postea, publica, etc., está siendo vigilado por las fuerzas de seguridad, podrá inhibirse de emitir, por ejemplo, opiniones críticas o disidentes, afectando la libertad de expresión, y perjudicando la calidad plural y democrática del debate público[2].

Además de ello, el ciberpatrullaje puede tener un efecto aún más grave sobre la libertad de expresión de los y las usuarios/as de las redes sociales al generar consecuencias penales sobre la base de afirmaciones o expresiones que pueden confundirse con posibles tentativas de delitos. Muestra de ello son los numerosos episodios que han ocurrido recientemente en los que las fuerzas de seguridad -junto con funcionarios del poder judicial- procedieron a utilizar la vía penal para castigar afirmaciones en las redes sociales, por considerar que las mismas atentaban contra la seguridad y el orden públicos[3].

En este sentido, la Comisión Interamericana de Derechos Humanos (CIDH) ha establecido que *"la imposición de sanciones por el abuso de la libertad de expresión bajo el cargo de incitación a la violencia (entendida como la incitación a la comisión de la prueba actual, cierta, objetiva y contundente de que la persona no estaba simplemente manifestando una opinión (por dura, injusta o per- turbadora que esta sea), sino que tenía la clara intención de cometer un crimen y la posibilidad actual, real y efectiva de lograr sus objetivos. Si no fuera así, se estaría admitiendo la posibilidad de sancionar opiniones, y todos los Estados estarían habilitados para suprimir cualquier pensamiento o expresión crítica de las autoridades que, como el anarquismo o las opiniones radicalmente*

[2] Penney, J., "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", disponible en https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case

[3] Sólo a título de ejemplo, pueden verse: https://www.jujuyalmomento.com/investigacion/incito-realizar-saqueos-jujuy-y-fue-detenido-e-imputado-la-justicia-n105037; https://www.ellitoral.com/index.php/id_um/232903-identificaron-a-dos-usuarios-de-twitter-por-instigar-saqueos-mi-sueno-es-reventar-un-coto-sucesos.html; https://www.elciudadanoweb.com/se-quisieron-hacer-los-vivos-y-los-detuvo-la-policia-por-instigar-saqueos/; https://www.chacohoy.com/noticias/view/223112; https://laverdadonline.com/detienen-a-un-juninense-por-incitar-a-saqueos-por-redes-facebook/; https://www.cronica.com.ar/policiales/Joven-incito-por-Facebook-a-saquear-comercios-en-la-cuarentena-y-acabo-detenido-20200402-0067.html; https://www.0223.com.ar/nota/2020-4-10-19-36-0-no-pudo-cobrar-los-10-mil-del-ife-e-incito-a-saquear-quedo-detenido.

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

contrarias al orden establecido, cuestionan incluso, la propia existencia de las instituciones vigentes"[4].

Y de hecho, las limitaciones a este tipo de expresiones también se encuentran establecidas por el Sistema Interamericano de Derechos Humanos (SIDH) en virtud del art. 13.2 de la Convención Americana de Derechos Humanos (CADH). Dicha norma, y en función de la práctica jurisprudencial de los organismos de la región, prevé el llamado test tripartito: las restricciones deben provenir de una ley clara y precisa; deben perseguir fines legítimos consagrados en la CADH; y deben ser necesarias (útiles, necesarias y estrictamente proporcionadas) en una sociedad democrática para alcanzar dichos fines[5].

Recientemente, la CIDH y la Relatoría Especial por la Libertad de Expresión manifestaron su preocupación por las violaciones a la libertad de expresión y restricciones al derecho a la información a raíz de las medidas establecidas por los Estados de la región en el marco de la respuesta a la pandemia[6].

Ambos organismos sostuvieron que algunos Estados recurrieron a figuras del derecho penal para sancionar la difusión de ideas e información calificadas como falsas o incitaciones al pánico respecto a la salud pública. Aún más, señalaron a la Argentina como uno de los casos identificados al sostener que *"en Argentina, se habrían iniciado causas penales por "intimidación pública"* contra al menos cinco personas que publicaron en sus redes sociales información que sería *crímenes, a la ruptura del orden público o de la seguridad nacional) debe tener como presupuesto* falsa". Y que *"tanto en Colombia como en Argentina se estarían realizando labores de "ciberpatrullaje", que tendrían como objetivo identificar cuentas que difundan información falsa"*.

A esto se le debe agregar la vigencia del estándar de *"peligro real y concreto"*, según el cual, aún cuando el Estado tiene un interés legítimo en prevenir la violencia y, por lo tanto, puede prohibir la difusión de ciertas ideas susceptibles de provocar actos de violencia, se debe analizar si efectivamente la difusión de dicha idea va a provocar actos de violencia.

Pero, justamente, el ciberpatrullaje por sí solo no permite hacer ese tipo de distinción contextual, por eso puede comprometer el estándar de peligro concreto: en el marco del ciberpatrullaje -tal como lo dijimos en el punto previo- es muy difícil identificar cuándo una expresión en una red social puede provocar ese peligro real y concreto que habilita el accionar de las fuerzas de seguridad.

Propuesta:

El protocolo debe tener criterios expresos sobre cómo identificará y procesará la información relevada de modo de poder distinguir, por ejemplo, entre meras afirmaciones aparentemente delictivas de

[4] CIDH, Relatoría Especial para la Libertad de Expresión. Marco jurídico interamericano sobre la li- bertad de expresión. OEA/Ser.L/V/II. CIDH/RELE/INF.2/09, 30 diciembre 2009, párr. 58

[5] Ibidem.

[6] http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2 . Al respecto se sostuvo que *"los relatores para libertad de expresión indicaron que los Estados no deberían establecer tipos penales para sancionar la difusión de desinformación o de noticias falsas. Ello, dado que la introducción de tipos penales podría retrotraer a la región a una lógica de criminalizar expresiones sobre funcionarios o asuntos de interés público y establecer una herramienta con un fuerte efecto inhibitorio de la difusión de ideas, críticas e información. (…) Por último, la CIDH y la Relatoría Especial han advertido en repetidas oportunidades sobre el uso de figuras penales vagas y ambiguas que no cumplen con los requisitos exigidos por el derecho internacional para criminalizar el trabajo periodístico, la defensa de los derechos humanos y las expresiones de crítica a través de redes sociales"*.

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

aquellas que efectivamente promuevan una situación de *"peligro claro y concreto"*. Debe, además, reconocer expresamente que actuará sólo ante la existencia de un peligro claro y concreto.

4. El derecho a la privacidad

Artículo 6º – Los cuerpos policiales y fuerzas de seguridad federales realizarán las tareas de ciberpatrullaje cumpliendo estrictamente los siguientes principios de actuación: (…) d. Protección de datos personales y privacidad. En el marco de la realización de actividades de ciberpatrullaje, el personal de los cuerpos policiales y fueras de seguridad federales deberán ajustarse estrictamente a lo normado en relación a la Ley 25.326 de Protección de Datos Personales, con especial atención a los datos considerados sensibles, es decir datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; y a las publicaciones efectuadas por niños, niñas y adolescentes.

Artículo 7º – La información obtenida en el desarrollo de las tareas de ciberpatrullaje consistirá en datos, imágenes, relatos, registros audiovisuales y testimonios recolectados en el curso del monitoreo y la observación de fuentes digitales abiertas acordes a la investigación del delito que se persigue. Se entenderá por "fuente digital abierta" a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley 25.326 de Protección de Datos Personales y sus normas reglamentarias.

Comentario:

La privacidad se define como el derecho de toda persona a tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otros y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados. El derecho a la privacidad también es la capacidad de las personas para determinar quién posee información acerca de ellos y cómo se utiliza dicha información que tienen las personas, esto es, el derecho a la autodeterminación informativa.

Como consecuencia de ello, y por más de que se estén monitoreando sus expresiones en la esfera pública, como pueden ser las redes sociales, las personas tienen una expectativa de privacidad en la que esperan que no se haga seguimiento de sus expresiones, no se haga recolección y no se haga tratamiento de esa información.

Aún cuando las redes sociales puedan ser reconocidas como "espacio público" esto no implica que los alcances del Estado en materia de investigación sean ilimitadas. No todo lo que ocurre en el espacio público -una conversación en la calle/en público, un intercambio en Twitter, son pasibles de investigación por parte del Estado. El ciberpatrullaje también exige criterios y reglas de transparencia y rendición de cuentas, así como superar el test de necesidad y proporcionalidad.

Amnistía Internacional no conoce ni se ha informado cómo se lleva adelante el ciberpatrullaje, qué tecnologías se cuentan para ello, así como tampoco con qué información se cruzan los datos obtenidos como para poder compartir sus observaciones puntuales.

En este orden de ideas, el Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo ha dicho lo siguiente: *"El artículo 17 dispone que, como mínimo, los Estados que utilizan tecnología de vigilancia a gran escala den cuenta pública y coherentemente de los beneficios tangibles que se derivan de su uso. Sin esa justificación, sencillamente no se puede evaluar la compatibilidad de esta nueva práctica de los*

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Estados con los requisitos del Pacto. (…) ***Para poder evaluar la legalidad de estas medidas es preciso, primeramente, que los Estados que usan esta tecnología sean claros respecto a su metodología y su justificación.*** *De lo contrario, se corre el riesgo de que la injerencia sistemática en la seguridad de las comunicaciones digitales siga proliferando sin que se analicen detenidamente las consecuencias del abandono general del derecho a la privacidad en línea. Si los Estados que usan esta tecnología monopolizan la información sobre sus consecuencias, imperará una forma de censura conceptual que impedirá que se mantenga un debate fundamentado"*[7].

Una de las consecuencias normativas del derecho a la intimidad es el llamado derecho a la autodeterminación informativa, esto es, el derecho que tiene toda persona a poder saber fehacientemente quién posee información suya, de dónde es obtenida ésta y con qué fines[8]. De allí que entendemos central aportar algunas consideraciones sobre la relación entre el ciberpatrullaje y la privacidad conforme lo previsto en la Ley de Protección de Datos Personales -Ley 25.326-, sobre todo teniendo en miras que los propios artículos citados prescriben que el ciberpatrullaje debe ajustarse a lo previsto en dicha ley.

Esta norma define a los datos sensibles como aquellos que *"revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"*(-art. 2)-. Esta ley, por su parte, establece un importante umbral de protección a estos datos: los incisos 2 y 3 del artículo 7 prescriben lo siguiente: *"Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley…"; y que "Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles (...).* "

Dicho de otro modo, las decisiones políticas que autoricen la recolección de datos sensibles deben cumplir con dos requisitos formales: que sea formalmente una ley -esto es, una decisión dictada por el Congreso de la Nación- y que esté sustentada en razones de interés general. Asumiendo que las presentes circunstancias excepcionales justifican ese interés general y, a su vez, la imposibilidad de tomar una decisión legislativa, aún resta otro requisito ya no formal, sino sustantivo: el ciberpatrullaje no puede terminar generando formación de archivos, bancos o registros.

Y aquí la tensión con el Protocolo es prístina toda vez que el propio artículo 7 citado previamente establece que *"La información obtenida en el desarrollo de las tareas de ciberpatrullaje consistirá en datos, imágenes, relatos, registros audiovisuales y testimonios recolectados en el curso del monitoreo y la observación de fuentes digitales abiertas acordes a la investigación del delito que se persigue"*. Es decir, la regulación en cuestión establece la formación de registros audiovisuales y la recolección de testimonios; que sólo pueden terminar en la formación de un archivo o un banco de información. Todas estas cuestiones están expresamente prohibidas por la Ley de Protección de Datos

[7] A/69/397, párrafo 14. El resaltado nos pertenece.

[8] De hecho la Comisión Interamericana de Derechos Humanos en su resolución 1/2020 expresó que entre los deberes del Estado en el marco del COVID se encuentra el de *"Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones"*.

AMNISTÍA INTERNACIONAL

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.:
contacto@amnistia.org.ar
W.: www.amnistia.org.ar

Personales. Por estas mismas razones, esta disposición también puede entrar en colisión con el artículo 8.a. del propio protocolo[9].

Propuesta:
Modificar la redacción del artículo 7 eliminando la posibilidad de formar registros y recolección de datos; de modo de establecer su adecuación con la Ley de Protección de Datos Personales. Se recomienda, asimismo, solicitar dictamen de la Agencia de Acceso a la Información Pública, el marco de sus competencias legales (Ley 27275 , art. 24, incisos k y t), sobre la posible afectación de sus prácticas de investigación con relación a la protección integral de datos personales.

5. La formación y capacitación de los agentes y funcionarios
Artículo 12º – El personal encargado del ciberpatrullaje deberá recibir formación acorde a las tareas, cuya currícula será coordinada y supervisada por el Ministerio de Seguridad de la Nación.

Comentario:
Si bien celebramos la inclusión de este artículo, entendemos que su redacción no es completa, puesto que deben establecerse políticas de formación y capacitación a los funcionarios y agentes que trabajen en estas tareas, pero es sumamente relevante que la misma tenga perspectiva de derechos humanos.

Propuesta:
Establecer que la formación y capacitación debe contemplar, expresamente, la perspectiva de derechos humanos.

6. Comentarios adicionales
Sin perjuicio de haber remarcado una serie de comentarios acerca del texto de Reglamento propuesto, entendemos que es necesario también agregar algunos puntos que han quedado excluidos del mismo, proponiendo, entonces, su incorporación en el cuerpo normativo del Anexo de la Resolución[10].

a. La publicidad: Los y las usuarios/as de las redes sociales deben saber que la policía, y otros organismos gubernamentales, recolectan información proveniente de fuentes abiertas y redes sociales –incluyendo todas las inferencias realizadas a partir de dichos datos–, para ejercer plenamente los derechos reconocidos por la Ley de Protección de Datos Personales (acceso, rectificación, supresión y actualización). Brindado a conocer los alcances y limitaciones, de modos de no causar autocensura (chilling effect) tal como fue anticipado.

[9] ARTÍCULO 8º – Se encuentra expresamente prohibido: a. Obtener información, producir inteligencia o almacenar datos sobre personas o usuarios por el sólo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.
[10] Al respecto puede verse Asociación por los Derechos Civiles, Seguidores que no vemos. Una primera aproximación al uso estatal del Open source intelligence (OSINT) y Social media intelligence (SOCMINT), disponible en https://adc.org.ar | https://adcdigital.org.ar

AMNISTÍA INTERNACIONAL

AMNISTÍA INTERNACIONAL ARGENTINA

Paraguay 1178
Piso 10º
C1057AAR
Buenos Aires

Tel.: +54 11 4811 6469
E.: contacto@amnistia.org.ar
W.: www.amnistia.org.ar

b. Rendición de cuentas: el protocolo debería estipular un sistema de rendición de cuentas, que establezca el deber de publicar regularmente información relacionada con: la cantidad de casos y personas investigadas junto con la duración de dichas actividades; las redes sociales –y sitios web en general– que fueron vigiladas; las herramientas y las metodologías utilizadas para cada caso investigado.

c. Responsabilidad por el uso abusivo y violatorio: El protocolo debe contener un sistema sancionatorio que penalice la vigilancia ilegal por parte de actores públicos o privados, con sanciones penales y civiles suficientes y adecuadas.

d. También se debe estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información.