Abril 2020

Sobre la necesidad de una ley para regular las técnicas de investigación en fuentes abiertas y redes sociales

Desde la Asociación por los Derechos Civiles (ADC) exponemos los siguientes lineamientos respecto al uso de técnicas de investigación de fuentes abiertas en internet y redes sociales con fines de persecución criminal, por parte de las fuerzas policiales y de seguridad.

El enfoque de nuestro aporte: La ADC entiende que el presente debate debe llevarse a cabo de manera amplia, robusta y participativa. Esto significa por un lado la necesaria intervención de todos los sectores que pueden ser alcanzados por las técnicas en cuestión. Por el otro, implica que la discusión no debe guiarse de manera exclusiva por el actual marco de emergencia sino que debemos tener en cuenta el estado de situación que puede consagrarse más allá de la misma. Finalmente, entendemos que un tratamiento unilateral de esta materia por parte del Poder Ejecutivo no satisface mínimos requisitos de legalidad. Por lo tanto, los aportes expuestos a continuación también serán compartidos con miembros del Poder Legislativo y otros actores centrales en la discusión.

Del mismo modo, nuestro aporte debe entenderse como insumo para un **debate legislativo**. **La discusión sobre la regulación de estas actividades no puede enmarcarse en un protocolo, disposición, resolución u otras normas de menor jerarquía.** Esta afirmación se funda, entre otros, en los artículos 19 de la Constitución Nacional y el art. 30 de la Convención Americana sobre Derechos Humanos. Y en el supuesto excepcional de considerarse el reemplazo de las normas legislativas por un DNU, entonces este último debería cumplir con los estrictos requisitos elaborados por la Corte Suprema de Justicia de la Nación. Nuestro máximo tribunal ha sostenido que para el caso para que el Presidente de la Nación pueda ejercer legítimamente las excepcionales facultades legislativas que,

en principio, le son ajenas, es necesaria la concurrencia de alguna de estas dos circunstancias: 1) que sea imposible dictar la ley mediante el trámite ordinario previsto por la Constitución, vale decir, que las cámaras del Congreso no puedan reunirse por circunstancias de fuerza mayor que lo impidan, como ocurriría en el caso de acciones bélicas o desastres naturales que impidiesen su reunión o el traslado de los legisladores a la Capital Federal; o 2) que la situación que requiere solución legislativa sea de una urgencia tal que deba ser solucionada inmediatamente, en un plazo incompatible con el que demanda el trámite normal de las leyes (Cfr. Fallos "Verrocchi" y "Consumidores Argentinos")

Acorde con lo que venimos señalando desde hace tiempo, **en tanto no exista un sustento legal proveniente del órgano legislativo, un protocolo de estas características no puede considerarse constitucional.**

Desde ya, un proyecto de ley para la regulación de estas actividades deberá contemplar mayores detalles de los aquí descritos y señalados. Asimismo, una discusión robusta requiere aportes que exceden el conocimiento jurídico. En particular, la participación de la comunidad técnica es fundamental para entender los alcances de las técnicas de investigación consideradas.

La emergencia y la libertad de expresión: Los organismos internacionales han emitido diversas pautas para evitar que la actuación estatal afecte de manera injustificada la vigencia de los derechos humanos. En la materia que nos ocupa, debemos prestar especial atención a la libertad de expresión, ya que las tareas de inteligencia en el ámbito digital en muchos casos se enfocan en actos discursivos.

En el sentido expuesto, recordamos que los relatores de libertad de expresión del sistema universal, sistema interamericano y la Organización para la Seguridad y la Cooperación en Europa, han manifestado que "*cualquier intento de penalizar la información relativa a la pandemia puede crear desconfianza en la información*

institucional, retrasar el acceso a información fiable y tener un efecto silenciador en la libertad de expresión".[1]

De este modo, el actual momento de excepción no puede ser un motivo para que el Estado incumpla el deber de garantizar que sus fuerzas de seguridad evitarán incurrir en actividades que impliquen una criminalización del discurso online, tal como ha sucedido hasta ahora en diversos casos.

Los delitos de intimidación pública y la criminalización del discurso online: Nos preocupa cualquier inclusión de los delitos de "intimidación pública" como una de las figuras penales a prestar atención. Como lo sostuvimos en anteriores comunicaciones, el tipo penal de los delitos de "intimidación pública" (art. 211 y 212 del Código Penal) es lo suficientemente abierto y ambiguo para afectar seriamente la libertad de expresión.

Al respecto, la Comisión Interamericana de Derechos Humanos (CIDH) y su Relatoría Especial para la Libertad de Expresión (RELE) nos recuerdan que "*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 l**as expresiones de crítica a través de redes sociales*** (el resaltado es nuestro)"[2]. En el caso argentino, la situación se agrava ya que la figura de "intimidación pública" ha sido utilizada precisamente para criminalizar el discurso online, cuestión que ha merecido la reciente preocupación del sistema interamericano.[3]

Por lo tanto, consideramos que el delito de "intimidación pública" no debe formar parte de las actividades de inteligencia en redes sociales. Asimismo, sugerimos que

[1] *COVID-19: Los gobiernos deben promover y proteger el acceso y la libre circulación de la información durante la pandemia - Expertos internacionales*, 19 de Marzo de 2020, disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1170&lID=2 (último acceso: 20/04/2020)
[2] *CIDH y su RELE expresan preocupación por las restricciones a la libertad de expresión y el acceso a la información en la respuesta de Estados a la pandemia del COVID-19*, disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2 (último acceso: 20/04/2020).
[3] Ibid.

cualquier disposición que manifieste el respeto a la libertad de expresión debe hacer referencia de manera expresa al estándar de que la conducta debe estar "*dirigida a incitar o producir una inminente acción ilegal y es probable que aquella incite o produzca tal acción*".[4] De esta manera, se reduciría la probabilidad de que la libertad de expresión se vea afectada.

Garantizar el derecho a la protesta en internet: Las restricciones a la libertad de manifestarnos en calles y plazas públicas implica que hoy exista un deber mayor del Estado de asegurar que internet sea un espacio libre y seguro para la protesta. Por lo tanto, garantías adicionales se requieren para cumplir la mencionada obligación. Entre ellas, debe establecerse expresamente la prohibición de recurrir a agentes infiltrados o con identidades falsas para vigilar a organizadores o participantes de protestas online.[5] Asimismo, recomendamos que se asegure la plena protección del discurso anónimo mediante la prohibición de recurrir a prácticas que apunten a levantar el anonimato, en tanto no haya orden y control judicial suficiente.[6]

Precisar la terminología: La adopción del término "ciberpatrullaje" debe ser revisada. Con el fin de brindar la mayor claridad posible para la implementación de cualquier regulación, debe evitarse el uso de un palabra que carece de antecedentes técnicos y asimila la vigilancia en internet al trabajo de las fuerzas policiales en las calles. En este sentido, el concepto correcto es "investigación en fuentes abiertas de datos y redes sociales", proveniente de las técnicas

[4] El estándar de la "acción ilegal inminente" ha sido creado por la Corte Suprema de los Estados Unidos de América (cfr. Brandenburg vs. Ohio, 1969) y fue adoptado por los tribunales argentinos para resolver casos de libertad de expresión. Para ver su aplicación a un caso de Internet, Sala I de la Cámara en lo Criminal Federal. *Causa Nro. 33.628 "Vita, Leonardo G. Y González Eggers, Matías s/procesamiento",* 13 de Marzo de 2002, disponible en http://www.hfernandezdelpech.com.ar/JurisprudenciaArgLiberExpreFalloCamaraFed.htm (último acceso: 20/04/2020).

[5] Cfr. Relatoría Especial para la Libertad de Expresión de la CIDH. *Protesta y Derechos Humanos Estándares sobre los derechos involucrados en la protesta social y las obligaciones que deben guiar la respuesta estatal* (Septiembre de 2019) párr. 300, disponible en https://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf (último acceso: 20/04/2020).

[6] Ibid, párr. 302

investigativas conocidas en inglés como "open source intelligence" y "social media intelligence".

Establecer un listado de tópicos: Nos preocupa cualquier regulación en donde no haya un catálogo de tópicos sobre los cuales va a recaer las tareas de inteligencia de fuentes abiertas y redes sociales. La resolución 31/18 establece en su art. 1 un listado específico de tópicos para las áreas de investigación de ciberdelitos. Sin embargo, el proyecto de reglamento ha eliminado estas especificaciones y en su lugar, ha dispuesto que las tareas policiales deberán ser para "*aquellos delitos que requieren la utilización de sistemas informáticos como medio comisivo accesorio o principal para su desarrollo*..." (art.3), "*delitos de acción pública*" (art. 4) o "*actividades que podrían revestir carácter ilícito*" (art. 4). De esta manera, se ha ampliado significativamente el campo de acción para llevar a cabo estas actividades.

Esta expansión entra en contradicción con los principios de legalidad y de proporcionalidad. El primer principio se ve afectado porque no hay un listado detallado de tópicos que delimiten de manera previa y cierta la actuación policial. El segundo principio se perjudica en tanto la ausencia de pautas específicas otorga un extenso margen de discrecionalidad para decidir los delitos que requerirán la utilización de estas técnicas.

Una acotación del catálogo de delitos ayudaría a orientar el accionar policial hacia aquellas actividades delictivas que efectivamente merecen ser investigadas, sin correr el riesgo de habilitar poder punitivo para conductas que consisten en la emisión de discurso. Por lo tanto, cualquier regulación debería incorporar un listado taxativo de aquellos tópicos que serán investigados por las fuerzas de seguridad mediante estas técnicas de investigación. La selección de los mismos deberá encontrarse fundada y revisarse periódicamente.

Asimismo, según la descripción brindada por los artículos 3 y 4 del reglamento, se orienta a las fuerzas policiales y de seguridad al uso de técnicas de investigación en fuentes abiertas para la "detección y prevención" de delitos, enmarcando a estas tareas como parte de la investigación preliminar del delito, que permite a las fuerzas "identificar, prevenir y alertar" la comisión de acciones tipificadas en el Código Penal.

Nos preocupa que este marco conceptual institucionalice y refuerce la discrecionalidad bajo la cual actúan las fuerzas policiales y de seguridad, al describir con ambos artículos lo que podemos definir como vigilancia masiva. La vigilancia masiva es la práctica por la cual se observa detenidamente a un grupo de personas o conjunto poblacional, de manera indiscriminada, sin una individualización de presuntos sospechosos por la comisión de tipos penales determinados.[7]

En este sentido, el abordaje para la regulación de la investigación en fuentes abiertas debe realizarse describiendo todos los escenarios posibles para precisar la procedencia ante cada supuesto. En primer lugar, distinguiendo las tareas que se realizan en el marco de causas judiciales, de aquellas actividades enmarcadas como "investigación preliminar". En segundo lugar, estipular concretamente los distintos escenarios de los tipos de tareas que pueden efectuarse, junto con la descripción de su metodología.

La asignación de cada tarea de investigación en fuentes abiertas debe estar delimitada por objetivos específicos, describiendo con precisión los supuestos generales delimitados por el artículo 5 del proyecto de reglamento.

[7] *Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance*, Christopher Parsons, Citizen Lab, 20 de octubre de 2015, disponible en: https://tspace.library.utoronto.ca/bitstream/1807/76113/1/beyond%20privacy%20articulating.pdf

Las órdenes de actuación deben fundar debidamente la proporcionalidad, dejando asentado por qué las tareas de investigación en fuentes abiertas son el medio adecuado para el fin perseguido.

Prohibiciones: Como parte de la regulación para limitar la injerencia en derechos fundamentales, deben incorporarse al menos dos nuevas prohibiciones:

a) El uso de bases de datos que han sido publicadas en internet como resultado de una filtración de información privada, en particular aquellas que contengan direcciones de email y contraseñas.
b) La creación de perfiles falsos para el ingreso a cuentas privadas. Lo cual solo puede proceder en el marco de una orden de juez competente bajo las figuras enmarcadas en el Código Procesal Penal, estipulando en la orden, como mínimo, el nombre de usuario del perfil creado, las cuentas en las que se solicitará ser seguidor o "amistad", el período de tiempo por el que se utilizará el usuario.

Capacitación y formación: Las instancias de profesionalización del personal a cargo de las tareas de investigación es pivotal para asegurar la correcta aplicación del reglamento. El entrenamiento que reciba el personal de cada fuerza policial y de seguridad debe contar con la enseñanza de nociones sobre el ejercicio de derechos humanos en el entorno digital (en particular privacidad, datos personales, libertad de expresión, reunión y asociación, protesta), que resulten en la total comprensión del impacto que presentan las técnicas de investigación y tareas de vigilancia en los derechos fundamentales.

Dentro de las pautas generales de actuación sugerimos también la incorporación de lineamientos claros que permitan dilucidar cómo se procederá en la determinación de la confiabilidad, veracidad y calidad de la información que es recolectada, procesada y almacenada. Estos lineamientos deben responder, por ejemplo, a interrogantes sobre ¿Cómo se distinguen e identifican expresiones que pueden ser delictivas en apariencia, pero son en realidad simples bromas o parte

del intercambio cultural y lenguaje que existe en internet? ¿Cuáles son los pasos que sigue un oficial a cargo de las tareas de investigación para corroborar la utilidad y legitimidad de la información que se recolecta? ¿Qué indicadores se utilizan para los criterios de investigación?

Transparencia y rendición de cuentas: Una regulación seria y democrática sobre las actividades de vigilancia estatal en internet, debe contar con bases sólidas de transparencia activa y mecanismos adecuados de supervisión.

El trabajo de cada fuerza policial y de seguridad debe ser realizado de una manera tal que permita la trazabilidad de todas las órdenes impartidas y decisiones tomadas, con el propósito de facilitar la transparencia activa de parte del Ministerio de Seguridad.

Las actividades de investigación en internet deben encontrarse acompañadas de una constante supervisión y análisis respecto a su utilidad en el marco de la política criminal definida. Para ello, proponemos la publicación regular de reportes de transparencia e informes de gestión, que contengan, como mínimo, información estadística objetiva y basada en evidencia, detallando la cantidad de casos y cantidad de personas investigadas; el marco temporal de duración de cada actividad; los sitios web y redes sociales que fueron vigiladas y su relación con los tipos penales vinculados a cada investigación; las herramientas y las metodologías utilizadas para cada caso investigado.

Finalmente, establecer canales robustos de supervisión permiten rendir cuentas a la ciudadanía en el cumplimiento de los objetivos planteados. En este sentido, debe considerarse el rol que puede cumplir una comisión especial en el Congreso ante la cual el Ministerio de Seguridad, como responsable de cada fuerza policial y de seguridad, deba aportar toda la información pertinente sobre las actividades desarrolladas para su evaluación.