Despliegue de prácticas OSINT por los Estados:

Recomendaciones para evitar abusos y violaciones a derechos humanos

La inteligencia de fuentes abiertas (en adelante “OSINT”, acrónimo de “Open Source Intelligence”) hace alusión a las prácticas de recopilación y análisis de información que es recogida a través de fuentes abiertas –que están disponibles públicamente- para darles una utilidad o propósito en específico. Cuando el propósito está relacionado con las actividades de seguridad y vigilancia estatal, la información se utiliza para el planeamiento de actividades defensivas (prevención de ataques) u ofensivas (organización de operaciones)

Este tipo de prácticas implementadas por parte de autoridades encargadas de la inteligencia y la seguridad pueden implicar una vulneración a los derechos humanos. A través de la investigación “Inteligencia basada en fuentes abiertas (OSINT) y Derechos Humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay” se ha documentado que algunas autoridades en la región de Latinoamérica realizan actividades de vigilancia y monitoreo de fuentes abiertas de información en internet -como redes sociales, chats abiertos, blogs, medios de comunicación y foros de discusión- de las personas para perfilarlas. Lo anterior se realiza, en general, al margen de la legalidad y en total opacidad.

Es necesario definir de forma clara las facultades de las instancias gubernamentales y establecer mecanismos de control, contrapesos, transparencia y rendición de cuentas, además de garantizar la implementación de las siguientes recomendaciones mínimas para la utilización de OSINT por parte del estado para fines de seguridad:

* Resulta imprescindible que toda acción del Estado en la materia cumpla el test tripartito desarrollado en el sistema internacional de derechos humanos para que cualquier medida de vigilancia sea legal, necesaria y proporcionada.

* La actividad de OSINT, incluso desde el Estado, puede tener usos legítimos, como los periodísticos, la formulación de políticas públicas o incluso de investigación criminal. Sin embargo, la falta de claridad respecto a las funciones que se ejercen al hacer OSINT desde el Estado (investigación, vigilancia preventiva o inteligencia) hace más posibles las violaciones de derechos. En ese sentido, es necesario definir de forma clara las facultades del Estado (entidades, situaciones y condiciones del uso) y establecer mecanismos de control para el uso de tecnologías como el OSINT.

- La regulación de la actividad debe contemplar la creación –por ley– de protocolos específicos que rijan la recolección, el procesamiento y la eliminación de información obtenida de fuentes abiertas. Dicha reglamentación deberá incluir qué tipo de datos se pueden recolectar en fuentes abiertas, y qué fines cumplirá la recolección; además, procurará proteger la privacidad de las personas usuarias y tolerar todas las expresiones permitidas por el marco jurídico local e internacional en materia de libertad de expresión.

- Los protocolos deberán prohibir la actividad de perfilamiento de personas. Además, se deberá exigir que, si se realiza vigilancia sobre una persona, ésta responda a una orden judicial debidamente fundada.

- Los protocolos deberán establecer principios de rendición de cuentas, como la publicación de reportes periódicos que señalen las prácticas que se realizaron en fuentes abiertas digitales. De la misma forma, el protocolo debe cumplir con los principios previstos por las leyes de protección de datos personales en los casos aplicables, para que los titulares de los datos puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición.

- Para evitar las violaciones de derechos en el uso de las técnicas OSINT son necesarios mecanismos de control. Algunos de ellos deben ser la notificación posterior a los ciudadanos que fueron vigilados con tecnologías y el uso que se dio a esa información, el control previo de jueces, y el establecimiento de sanciones claras para quienes cometan abusos.

- Deben establecerse obligaciones de transparencia y apertura en la contratación de tecnología o servicios de terceros que incluyen esta práctica. Es necesario conocer los contratos existentes entre Estados y empresas privadas proveedoras de servicios OSINT, los cuales deberían ser ampliamente difundidos y encontrarse fácilmente disponibles, así como la información acerca de la asignación de recursos y el gasto realizado para esas tareas.

- Debe exigirse la publicación de estadísticas acerca de las instancias específicas en las que se realizó OSINT sobre particulares y, cuando ello sea posible, los motivos que las justificaron.

- Otro aspecto a mejorar en la transparencia de los gobiernos es el recurrente uso de las razones de seguridad nacional como valla para el acceso a la información pública.

- Que la actividad sea tercerizada por el Estado en un sujeto no estatal, no releva a aquél de ninguna obligación en materia de derechos humanos.

- Por último, se impone requerir a aquellos Estados que contratan sistemas o servicios de OSINT, que realicen estudios de impacto en materia de privacidad, y que sus resultados sean también ampliamente difundidos.

Para mayor información consultar:

sitio web informe regional