Libertad de Expresión en el Ámbito Digital

El estado de situación en América Latina

Resumen ejecutivo

Capítulo III

Vigilancia estatal de las comunicaciones

por los Derechos Civiles

Área de Libertad de Expresión

Septiembre 2016

adc.org.ar | adcdigital.org.ar

El presente documento es un resumen elaborado por ADC del capítulo *Vigilancia estatal de las comunicaciones* del informe *Libertad de Expresión en el Ámbito Digital. El estado de situación en América Latina*, el cual fue redactado por *Fundación Karisma*. La versión completa de este capítulo puede ser consultada en https://adcdigital.org.ar/wp-content/uploads/2016/04/LibEx-en-LatAm-AmbitoDigital.pdf, páginas 70 a 94.

El informe tuvo como objetivo hacer un relevamiento de la situación a nivel regional de diversos aspectos vinculados a la libertad de expresión online, analizando legislación, proyectos de ley y casos jurisprudenciales hasta diciembre de 2015. Su objetivo es servir de guía para impulsar el debate dentro de cada país y aportar lineamientos para una implementación legislativa respetuosa de los derechos de las personas en Internet.

Vigilancia estatal de las comunicaciones

Importancia del tema: estado actual

1. La vigilancia estatal de las comunicaciones busca recolectar datos para tareas de inteligencia o investigación criminal. Sin embargo, un mal uso de las mismas puede causar graves afectaciones a los derechos humanos de las personas.

2. La falta de un proceso democrático y la ausencia de controles y medidas de transparencia provoca que la actividad de vigilancia se desenvuelva en el campo de la ilegalidad.

3. El peligro es que los gobiernos utilicen las herramientas de vigilancia para ejercer actividades de espionaje sobre toda la población o para la persecución de opositores políticos.

4. Las nuevas tecnologías permiten expandir enormemente la capacidad de vigilancia de los Estados, ya que los nuevos desarrollos de software han permitido que se pueda acceder subrepticiamente a todos los dispositivos electrónicos y obtener información de ellos de una manera sencilla.

5. Las medidas de retención de datos de las comunicaciones constituye una de las acciones más utilizadas por los gobiernos para ejercer su tarea de vigilancia. Sin embargo, su mala utilización puede acarrear consecuencias negativas para el derecho a la privacidad o a la libertad de expresión de las personas.

6. Se ha registrado un uso creciente de metadatos (aquellos que se refieren al origen, destino, fecha, hora, y duración de la comunicación) para vigilancia, los cuales pueden hacernos conocer más sobre una persona que el mismo contenido de la comunicación, y por lo tanto, genera conflictos con el derecho a la privacidad.

Estándares a aplicar

- Relatoría Especial para la Libertad de Expresión: La legitimidad de las medidas de vigilancia de las comunicaciones derivan del cumplimiento de las siguientes condiciones: consagración legal; búsqueda de una finalidad imperativa; necesidad, idoneidad y proporcionalidad de la medida; debido proceso y reserva judicial.

  Por otro lado, el uso de programas y sistemas de vigilancia debe: estar establecido de manera clara y precisa en la ley; ser verdaderamente excepcional y selectivo; estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos, como la investigación de delitos graves previstos en la legislación.

- Principios Internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones: Legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas; garantías para la cooperación internacional y contra el acceso ilegítimo, y derecho a un recurso efectivo.

La situación en América Latina

Las leyes sobre retención de datos son demasiado permisivas, amplias y poco respetuosas de las garantías de los derechos humanos.

- Perú: El Decreto Legislativo 1182, que regula la retención de datos, es demasiado abierta, ya que no precisa qué entiende por "datos derivados de las telecomunicaciones" ni establece qué comprenden los datos de localización. Además, no existe claridad respecto a las autoridades que pueden acceder a los datos ni una determinación de las condiciones de acceso a los mismos. Por otro lado, cuando la Policía solicita acceso a los datos de tráfico no se requiere autorización judicial previa.

- México: El acceso a datos de tráfico retenidos en virtud de la Ley Federal de Telecomunicaciones y Radiodifusión, y a datos de geolocalización no requiere autorización judicial. Asimismo, se establece que dichos datos pueden ser entregados a las "autoridades competentes", sin establecerse claramente cuáles son.

- Colombia: La normativa habla de retener el "historial de comunicaciones" sin especificar qué se entiende por ello. Además, se permite la obtención de "cualquier otra información" que contribuya a la localización de la persona en cuestión. Asimismo, no hay limitación respecto a los delitos cuya investigación puede servirse de datos retenidos. Finalmente, el acceso a los datos o a la geolocalización no requiere autorización judicial ni está sometido a control posterior.

- Brasil: la legislación no especifica el tipo de investigación que amerita el acceso a los datos retenidos. Tampoco se determina las autoridades que pueden acceder a este tipo

de información. No existe claridad respecto a la necesidad de requerir autorización judicial para acceder a los datos.

- Argentina: Actualmente no existen leyes expresas sobre retención de datos, aunque existe un reglamento de calidad de servicio que obliga a los prestadores a conservar datos que recojan sus sistemas. La ley 25.873 obligaba a los prestadores de servicios de telecomunicaciones a retener datos y registros de tráficos de los usuarios por un plazo de 10 años. Sin embargo, esta normativa fue declarada inconstitucional por la Corte Suprema, ya que violaba los requisitos de legalidad (no dejaba en claro qué son datos de tráfico) , necesidad (no basta invocar el interés general) y proporcionalidad (el plazo de 10 años fue considerado amplísimo y excesivo).

Utilización de herramientas de hackeo en actividades de vigilancia estatal: compra de software de vigilancia por parte de los gobiernos para realizar actividades de espionaje (Caso Hacking Team: México, Chile, Panamá, Colombia, Ecuador y Honduras). En ninguno de los países está prevista legalmente la actividad del hackeo de dispositivos. La normativa que autorice el hackeo debe ser clara respecto al tipo de herramienta que se debe usar, las funciones del equipo que puede afectar y el plazo durante el cual puede ser empleada.

Conclusiones y recomendaciones

- Actualmente ningún régimen de retención de datos en América Latina cumple con todos los estándares legales que se deben respetar.

- Toda medida de retención de datos debe ser ordenada y controlada por una autoridad judicial independiente.

- Se debe equiparar protección de los metadatos a los resguardos que se intenta dar a los datos.

- La retención de datos debe tener un carácter residual frente a otras técnicas menos invasivas.

- El hackeo debe requerir autorización judicial, a través de un procedimiento en el que se pueda comprobar la satisfacción de los requisitos legales (observación de la cadena de custodia, notificación de la persona afectada y presentación de informes de transparencia).

- En aquellos países que regulen legislativamente la utilización de técnicas de recolección de datos y debido a su carácter fuertemente invasivo en la privacidad de las personas, la normativa debe cumplir con los principios de legalidad, necesidad y proporcionalidad. Asimismo, deben explicitar claramente el motivo, el modo, el destinatario y el plazo de la medida.

- Para el caso de herramientas de hackeo, la legislación debe ser clara respecto a los tipos de herramientas que se pueden usar y las funciones del equipo que se pretende afectar. Asimismo, debe contener precisiones respecto a cuánto tiempo puede emplearse, bajo qué condiciones y ante qué autoridad se puede hacer.