

DERECHO A LA INTIMIDAD / PRIVACIDAD

Balance de las recomendaciones anteriores

Durante la revisión anterior de Colombia en el segundo ciclo, en 2013, no se menciona la intimidad (o privacidad) en el contexto de la protección de datos ni de la vigilancia de las comunicaciones en ninguna recomendación. Las reiteradas preocupaciones del Comité de Derechos Humanos de la ONU en relación con las políticas y prácticas ilegales de vigilancia de la comunicaciones en el país, expresadas en sus informes de 2010 y 2016, demuestran la importancia de que en este ciclo se adopten recomendaciones sobre estos temas.

Desafíos

Falta de garantías y controles a las actividades de vigilancia estatal y la retención de datos:
Aunque son actividades propias de un estado de derecho que buscan garantizar la seguridad nacional y el orden público, la vigilancia de las comunicaciones y la retención de datos de comunicaciones tienen un alto impacto en el ejercicio de derechos humanos. Esto obliga a los Estados a tener un marco legal con límites claros y precisos. Además, las actividades a autorizarse precisan de una evaluación acorde a criterios de necesidad, idoneidad y proporcionalidad. Esto no sucede en Colombia. La Ley de Inteligencia y Contrainteligencia y el nuevo Código de Policía confieren facultades ambiguas de vigilancia a las diferentes autoridades y no establecen mecanismos de control efectivo para estas actividades. Los mecanismos existentes no operan, como ocurre con la revisión y depuración de archivos de inteligencia.

Unidades del Ejército colombiano (GAULA) realizaron casi 2.000 interceptaciones ilegales a las líneas telefónicas de la Asociación de Familiares de Detenidos Desaparecidos (Asfaddes), y dos miembros fueron desaparecidos al parecer por paramilitares.

Desde la década de 1990 la antigua agencia de inteligencia del Estado interceptó las comunicaciones de periodistas, políticos, magistrados y defensores de derechos humanos, actividad que se conoce popularmente como “chuzadas”. La información obtenida se usó para alimentar archivos de inteligencia sobre estas personas, que hoy en día siguen sin depurarse. En 2013 el Fiscal General suspendió la plataforma de monitoreo de comunicaciones para investigaciones judiciales (PUMA), ante dudas sobre si la forma como se gestionaba la plataforma cumplía con la ley.

En 2014 se desenmascaró una operación fachada de inteligencia militar, denominada Andrómeda. Desde ahí, se vigilaban las comunicaciones digitales de políticos y periodistas relacionados con el proceso de paz entre el Gobierno colombiano y la guerrilla de las FARC en Cuba.

De otra parte, no es claro qué tipo de capacidades y tecnologías de vigilancia posee el país. Varios investigaciones han dando cuenta de un sistema que difiere sustancialmente de lo que está indicado en la ley. Además, mientras que la adquisición de tecnología de vigilancia no está regulada en el país, tecnologías muy invasivas parecen estar usándose por las autoridades con propósitos que van desde la investigación criminal hasta la supresión de la disidencia, pasando por la recopilación de información para inteligencia.

En 2015, filtraciones de las comunicaciones de la empresa italiana Hacking Team, mostraron que la Policía colombiana negociaba la adquisición de un sistema de control remoto para acceder a dispositivos electrónicos y obtener información almacenada en estos dispositivos.

Desafíos

Falta de Mecanismos de supervisión de las actividades de vigilancia estatal:

Para la vigilancia de comunicaciones en el marco de una investigación criminal, cualquier autoridad debe solicitar la autorización de interceptación ante un Juez. Pero esto no sucede cuando esta misma autoridad desea conocer los metadatos [1] de las comunicaciones, o cuando quien busca esa información es un organismo de inteligencia.

[1] Los metadatos son la información sobre las comunicaciones. Esto comprende hora de llamada, números marcados, duración de la llamada y localización geográfica a partir de la ubicación de las torres de telefonía.

Inadecuada protección de metadatos de las comunicaciones:

Desde hace años, la ley colombiana obliga a la retención de datos que generan las conexiones de telefonía fija, celulares o de internet por un periodo de cinco (5) años. Esto es problemático cuando se considera que el análisis de datos en su conjunto permite conocer los hábitos, preferencias y actividades de una persona, lo que potencialmente puede vulnerar más seriamente el derecho a la intimidad que el conocimiento del contenido de las comunicaciones. Además, el Gobierno colombiano no ha cumplido con la obligación de armonizar esta normativa con la nueva ley de protección de datos.

Por ejemplo, la Comisión de Regulación de Comunicaciones y el Ministerio de las TIC han implementado sistemas informáticos de recolección y almacenamiento masivo de datos y metadatos de la ciudadanía con la excusa de combatir el hurto de celulares o facilitar trámites electrónicos con el Estado. No existen mecanismos de protección o de control para el uso de los datos que recogen estos sistemas, lo que facilita el uso indebido para actividades de inteligencia.

Conceptos de privacidad y espacio público:

El nuevo Código de Policía limita la definición de privacidad, mientras amplía el concepto de espacio público para incluir, por ejemplo, al espectro electromagnético. Con base en este nuevo marco, se puede interpretar que las comunicaciones que viajen por el espectro se encuentran en el espacio público y por lo tanto pueden ser interceptadas.

Recomendaciones

1. Ajustar toda la normatividad sobre vigilancia de las comunicaciones a las normas internacionales de derechos humanos, especialmente al artículo 17 del Pacto Internacional por los Derechos Civiles y Políticos, y al artículo 12 de la Declaración Universal de Derechos Humanos para que todas las actividades de vigilancia de las comunicaciones cumplan los criterios de legalidad, necesidad y proporcionalidad, haciendo efectivo el derecho a la privacidad.

2. Derogar los reglamentos actuales sobre retención de datos de las comunicaciones, por violar el requisito de legalidad establecido en el artículo 17 del Pacto Internacional por los Derechos Civiles y Políticos y el artículo 12 de la Declaración Universal de Derechos Humanos.

3. Aplicar las medidas contenidas en la Ley de inteligencia relacionadas con revisión y depuración de archivos, y modificar esta norma para adoptar nuevos controles y supervisión a las operaciones de los organismos de inteligencia, incluidas las actividades de vigilancia, por un mecanismo de control independiente en el que participen las organizaciones de la sociedad civil.

4. Derogar las disposiciones del Código de Policía que afectan injustificadamente el derecho a la intimidad, especialmente las medidas relacionadas con la vigilancia masiva con cámaras, la definición de privacidad y la del espectro electromagnético como un espacio de intervención de la policía sin control judicial, para cumplir con el artículo 17 del Pacto Internacional por los Derechos Civiles y Políticos y el artículo 12 de la Declaración Universal de Derechos Humanos.