



## Derecho a la privacidad

20

### Balance de las recomendaciones anteriores

En el EPU previo no se formularon a Colombia recomendaciones relacionadas con el derecho a la intimidad. Sin embargo, países como Bután y Azerbaiyán recomendaron trabajar en eliminar las brechas de implementación de los derechos humanos en el país. También, relacionado con el tema, la República de Corea recomendó aumentar los esfuerzos para mejorar la transparencia estatal. De igual forma son múltiples los países (Alemania, Bolivia, Austria, Bélgica, Noruega) que se refirieron a tomar medidas para proteger a activistas y defensores de derechos humanos.

A pesar del llamado general por el respeto a los derechos humanos y la implementación de medidas de transparencia, en lo que tiene que ver con el derecho a la intimidad existe un problema serio debido a la falta de regulación de tecnologías que permiten la vigilancia a la ciudadanía.

### Desafíos

Continúan presentándose casos de perfilamientos a periodistas y activistas. Durante el último periodo de evaluación se han presentado varios casos de perfilamientos a activistas o periodistas haciendo uso mixto de herramientas de vigilancia analógicas y tecnológicas. Casos como los de las Carpetas Secretas (1) o los perfilamientos a periodistas como María Camila Villamizar (2) usando tecnología de inteligencia en fuentes abiertas de información (OSINT) (3), la cual permite recolectar y clasificar información publicada en internet, ponen de presente la continuidad en los casos de vigilancia a la sociedad civil por parte del Estado.

El Estado ha implementado tecnología que permite vigilancia masiva sin un marco legal claro. Tanto durante la pandemia del Covid-19 (4), como durante las protestas sociales de 2021 (5), la Policía en Colombia y el Ministerio de Defensa adelantaron labores de “ciberpatrullaje”, el cual consistía en un monitoreo en vivo del contenido publicado por la sociedad civil, el seguimiento de tendencias en redes sociales y el etiquetado como falso de algunas de las publicaciones de la población (6).

(1) El Espectador. Las “carpetas secretas” de inteligencia militar: ¿a quién iban dirigidas y para qué?. Disponible en: <https://www.elespectador.com/judicial/las-carpetas-secretas-de-inteligencia-militar-a-quienes-iban-dirigidas-y-para-que-article-917751/> y Semana. Las carpetas secretas. Disponible en: <https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/>

(2) Fundación para la Libertad de Expresión (FLIP). Inteligencia Militar incrementa su capacidad para vigilar a periodistas y ciudadanía con tecnología de fuentes abiertas. Disponible en: <https://www.flip.org.co/index.php/es/publicaciones/informes/item/3007-inteligencia-militar-incrementa-su-capacidad-para-vigilar-a-periodistas-y-ciudadania-con-tecnologia-de-fuentes-abiertas>

(3) La inteligencia de Fuentes Abiertas (OSINT por sus siglas en inglés) consiste en una serie de técnicas para recolectar y analizar datos que se encuentren alojados en fuentes de información de libre acceso con fines ofensivos o defensivos (planeación de operaciones). Para más información revisar: Karisma. Cuando el Estado vigila. OSINT y Ciberpatrullaje en Colombia. Disponible en: <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>

(4) Índice de Derechos Digitales. Ciberpatrullaje de la Policía Nacional para identificar desinformación. 2023. Disponible en: <https://indicederechos.digital/docs/CiberpatrullajeDesinformacion/>

(5) Fundación Karisma. Pistolas vs Celulares. Disponible en: <https://web.karisma.org.co/pistolas-contra-celulares/>

(6) Este tipo de actuaciones se dieron a conocer a través de los Balances Generales que eran publicados periódicamente por MinDefensa. Este es el correspondiente al 27 de junio de 2021: [https://www.google.com/url?sa=t&rct=j&u=https%3A%2F%2Fwww.mindefensa.gov.co%2Ffirj%2Fgo%2Fkm%2Fdocs%2FMindefensa%2FDocumentos%2Fdescargas%2Festudios\\_lectorales%2Finfo\\_estadistica%2FinformeCorrido\\_Balance\\_Paro\\_2021.pdf&usg=AOvVaw0YdrW5-0VaAUJo1fDYRN2U&opi=89978449](https://www.google.com/url?sa=t&rct=j&u=https%3A%2F%2Fwww.mindefensa.gov.co%2Ffirj%2Fgo%2Fkm%2Fdocs%2FMindefensa%2FDocumentos%2Fdescargas%2Festudios_lectorales%2Finfo_estadistica%2FinformeCorrido_Balance_Paro_2021.pdf&usg=AOvVaw0YdrW5-0VaAUJo1fDYRN2U&opi=89978449)

No hay una legislación que regule la adquisición y uso de tecnologías para la vigilancia. Entidades como el Ejército Nacional, la Dirección Nacional de Inteligencia, la Policía y la Fiscalía cuentan con herramientas para realizar monitoreo de contenido en internet, las cuales usan con fines como inteligencia, vigilancia o investigación judicial, sin que sea posible para la ciudadanía saber cuándo sucede y en aplicación de qué ley (7).

Estas adquisiciones se suman a otras de tecnologías, por ejemplo, Jammers (inhibidores de señales) (8), con las cuales es posible bloquear las señales de internet o telefonía de equipos, o los softwares SINGINT (Inteligencia de señales) (9) para interceptar señales, las cuáles adquieren de forma confidencial argumentando “seguridad nacional” y respecto de las cuales no es posible conocer cómo están siendo usadas y qué controles se aplican. Como resultado, distintas organizaciones de la sociedad civil han manifestado de forma pública las dificultades para acceder a información sobre la contratación de tecnología del Estado y respecto de la ineffectividad del derecho al acceso a la información en este ámbito (10).

Continúa la impunidad en casos de vigilancia y garantías al ciudadano. Persiste la impunidad respecto de los casos de perfilamientos o interceptaciones ilegales contra ciudadanos, periodistas y activistas por parte del Estado. No existen avances en las investigaciones internas y judiciales, sanciones ni reparaciones por los actos cometidos.

(7) Karisma. Cuando el Estado vigila. Osint y ciberpatrullaje en Colombia. Disponible en: <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia>

(8) Carolina Botero. La Silla Vacía. El misterio detrás de los cortes de internet en Cali durante el paro de 2021. Disponible en: <https://www.lasillavacia.com/historias/historias-silla-llena/el-misterio-detras-los-cortes-de-internet-en-cali-durante-el-paro-de-2021/>

(9) ODIN. Osint e Inteligencia. Qué es SIGINT, Cómo se usa y ejemplos de la inteligencia de señales. Disponible en: <https://odint.net/sigint/>

(10) Karisma. La punta del iceberg. Los problemas de transparencia del OSINT en Colombia. Disponible en: <https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/>

## Recomendaciones

1. Formular una regulación para las formas de adquisición, uso y control de tecnologías que tengan potencial de afectar derechos de la ciudadanía.
2. Intensificar el esfuerzo Estatal para investigar y perseguir a los funcionarios públicos involucrados en casos de vigilancia o interceptaciones ilegales a ciudadanos.
3. Formular una regulación que permita distinguir, de forma clara, qué función ejerce una entidad estatal al usar determinada tecnología y su obligación de notificar a la ciudadanía involucrada.
4. Asegurar que el uso de tecnologías de vigilancia cumpla con los principios de legalidad, legitimidad del fin, necesidad, proporcionalidad y no discriminación y que no anule el núcleo esencial del derecho.
5. Realizar análisis de impacto de derechos cuando adquiera y emplee tecnologías de vigilancia y debe considerar los riesgos de abuso de la tecnología.