GUÍA PARA PROTEGERTE DIGITALMENTE DURANTE UNA PROTESTA

Dejusticia

Fundación Karisma

Si vas a salir a protestar, debes conocer tus derechos. Además de saber qué hacer si te detienen injustamente o cómo denunciar agresiones, es importante tener claro cómo protegerte de la vigilancia policial.

En esta guía, la Fundación Karisma y el Centro de estudios Dejusticia, con el apoyo de Privacy International, ofrecemos información básica sobre las capacidades de vigilancia que tiene la policía colombiana y te damos algunos consejos para evitarla durante la protesta.

Aquí encontrarás definiciones, explicaciones y recomendaciones sobre la vigilancia a los dispositivos tecnológicos, las comunicaciones, la identidad y las redes sociales de las personas que protestan.

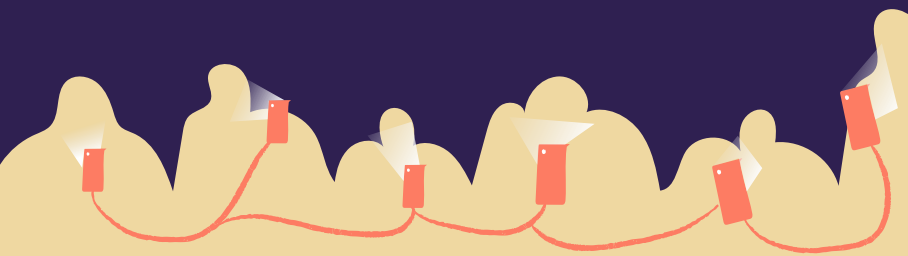


TABLA DE CONTENIDOS

I TUS DISPOSITIVOS

1.
¿Cómo puede acceder la policía a tus datos?

Tus datos pueden estar almacenados en tu celular o en la nube, por lo que La policía tiene herramientas para extraer información de ambos lugares.

Herramientas de extracción de datos de celulares

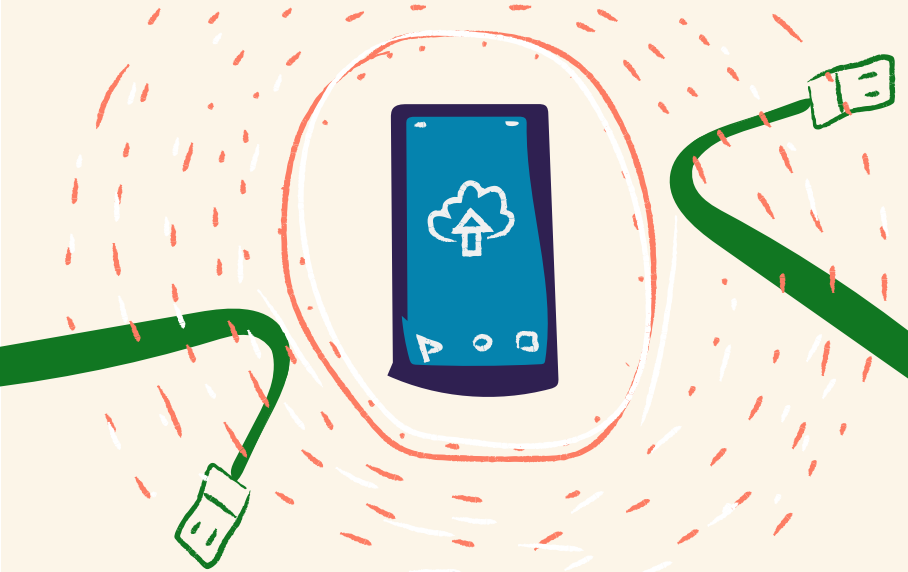
Son dispositivos o programas que le permiten a la policía extraer datos de los teléfonos celulares, incluyendo:

- contactos
- datos de llamadas (a quién llamas, cuándo y durante cuánto tiempo).
- mensajes de texto (a quién envías mensajes y cuándo).
- archivos (fotos, vídeos, audios, documentos, etc.).
- datos de aplicaciones
- historial de localización
- conexiones a redes wifi utilizadas (que pueden revelar la ubicación de cualquier lugar donde te hayas conectado a wifi, como tu lugar de trabajo o una cafetería).

Herramientas de extracción de datos en la nube

Esta tecnología le permite a la policía acceder a los datos almacenados en tu nube a través de tu celular. Algunos ejemplos de aplicaciones que almacenan datos en la nube son Google, Slack, Instagram, Telegram, Twitter, Facebook y Uber.

Toda esta información podría utilizarse para identificar a las personas que participan en la protesta, saber dónde están y qué hacen. Para extraer esos datos, la policía tendría que acceder físicamente a tu celular.



2. ¿Por qué esto afecta tus derechos?

Tu información personal, tanto en la nube como en tu teléfono celular, está protegida por el derecho fundamental a la intimidad. La policía no puede quitarte el teléfono, ni tú tienes la obligación de entregarlo.

La policía solo puede acceder a tus dispositivos en el marco de una investigación penal y con una orden escrita de un fiscal competente. En todo caso, un juez deberá revisar la legalidad del procedimiento en las siguientes 24 horas.

La policía también puede pedirte que enseñes el número IMEI* para comprobar que el dispositivo no sea robado, pero no estás en la obligación de entregarle tu teléfono.

Si un policía te pide tu IMEI, marca *#06#. Al hacerlo, aparecerá en tu pantalla y podrás mostrarlo sin que nadie manipule tu celular.

* El IMEI es un identificador internacional de todo teléfono celular. Es el equivalente a la cédula de los teléfonos celulares. Este número permite verificar si un teléfono ha sido reportado como robado y facilita desactivarlo incluso si se cambia la tarjeta SIM.

3. Consejos para proteger tus dispositivos en una protesta

- Mantén tu celular apagado o bloqueado con clave. Esto dificulta la extracción de datos.
- Mantén el sistema operativo de tu teléfono (Android o iOS) actualizado.
- Si es una opción para ti, considera dejar el celular en tu casa.
- En la sección de configuración de las aplicaciones que utilizas, desactiva la copia de seguridad (backup) en la nube.
- Cierra la sesión de todas las aplicaciones que no necesites.
- Comunícate a través de aplicaciones que tengan cifrado de extremo a extremo, como WhatsApp o Signal.
- Mientras no lo necesites, desactiva la opción de que aplicaciones como Google, Uber, Twitter, WhatsApp y Facebook accedan a tu ubicación.
- Elimina con frecuencia los chats, fotos, videos, contactos, historiales y otra información de tu celular (puedes hacer copias de seguridad en tu computador).

II TUS COMUNICACIONES

1. ¿Cómo puede acceder la policía a tus comunicaciones?

La policía tiene dos maneras de interceptar tus comunicaciones cuando usas la red de telefonía celular: mediante IMSI catchers y mediante accesos concedidos por las compañías telefónicas.

» *IMSI Catchers*

¿Qué es el IMSI?

Es un número único asociado a la tarjeta SIM que sirve para identificar al suscriptor de un teléfono celular. Se llama IMSI por ser la sigla del inglés international mobile subscriber identity.

¿Qué es un IMSI catcher?

Los IMSI catcher son dispositivos que simulan ser una torre de telefonía móvil y "engañan" a los celulares cercanos para que se conecten a él. Esto les permite interceptar las llamadas, mensajes de texto y la ubicación de una persona usuaria sin que esta lo sepa. Incluso, pueden usarse para controlar o bloquear llamadas y mensajes de texto o editar y enviar estos últimos haciéndose pasar por ti.

¿Cómo puede usarlos la policía en una protesta?

Pueden instalarlos en el lugar de la protesta para identificar los celulares que estén alrededor y eventualmente interceptar y alterar las comunicaciones.

» *Interceptaciones a través de compañías telefónicas*

¿Cómo funciona en Colombia?

Las autoridades judiciales y de inteligencia tienen equipos especiales y están facultadas para acceder a las comunicaciones que haces a través de las redes de las compañías telefónicas. Por ejemplo:

- El contenido de las comunicaciones.
- La ubicación de los dispositivos.
- El historial de llamadas y mensajes de texto.
- La duración de las llamadas telefónicas.

2. ¿Por qué esto afecta tus derechos?

Estos procedimientos en el marco de una protesta le permiten a la policía conocer quiénes son los manifestantes, qué dicen y dónde se encuentran, vulnerando la posibilidad de protestar anónimamente y aumentando los riesgos de persecución y perfilamiento.

3. Consejos para proteger tus comunicaciones durante la protesta

- Mantén tu celular en modo avión o apágalo por completo. Esto evita que un IMSI catcher pueda rastrear tu ubicación y tus comunicaciones.

- Evita hacer llamadas y enviar mensajes de texto por tu operador de telefonía celular. Si vas a hacer llamadas y enviar mensajes, hazlo por aplicaciones.

- Comunícate mediante aplicaciones que utilizan cifrado de extremo a extremo, como Signal o WhatsApp. Un IMSI catcher o la compañía telefónica solo registraría el uso de estas aplicaciones, no su contenido.

III TU IDENTIDAD

1. ¿Cómo puede la policía acceder a tu identidad?

La policía usa tecnología de reconocimiento facial para identificar a las personas a partir de las fotografías o videos tomados durante las protestas.

Las imágenes pueden venir de cámaras corporales, drones, cámaras de videovigilancia y de publicaciones en medios de comunicación y redes sociales.

» *Tecnología de reconocimiento facial*

¿Qué es?

El reconocimiento facial es un método que busca identificar o verificar la identidad de las personas utilizando capturas fotográficas o en video del rostro. Para que funcione es necesario contar con una base de datos que contenga registros faciales de las personas.

Con la foto de la persona se crea una "huella facial", es decir, una representación digital del rostro que se compara con los registros en la base de datos.

¿Cómo puede la policía usar esta tecnología durante una protesta?

La policía cuenta con un Sistema Automatizado de Identificación Biométrica (ABIS), conectado con la base de datos de identificación biométrica de la Registraduría. Esto les permite identificar a personas en videos e imágenes sin su autorización.

En 2019, un día antes del inicio de las protestas del 21N, la policía anunció en medios de comunicación que un helicóptero equipado con tecnología de reconocimiento facial sobrevolaría Bogotá para identificar a las personas que se manifestaran violentamente. Sin embargo, no hay evidencia de que alguien haya sido judicializado como resultado del uso de esta herramienta y, al parecer, se trató de una acción dirigida a disuadir a la ciudadanía de salir a protestar.

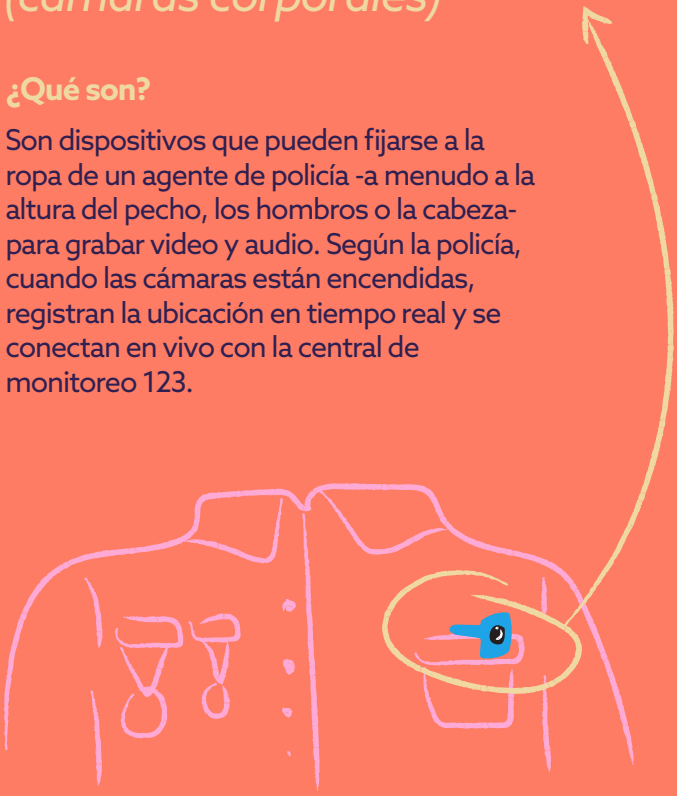
¿Por qué esto afecta tus derechos?

El uso de tecnologías de reconocimiento facial durante protestas afecta los derechos de reunión y a la libertad de expresión de los manifestantes, pues desincentiva la participación de la ciudadanía. Además, se puede prestar para perfilamientos y persecuciones ilegales.

» *Body Cams (cámaras corporales)*

¿Qué son?

Son dispositivos que pueden fijarse a la ropa de un agente de policía -a menudo a la altura del pecho, los hombros o la cabeza- para grabar video y audio. Según la policía, cuando las cámaras están encendidas, registran la ubicación en tiempo real y se conectan en vivo con la central de monitoreo 123.



¿Cómo puede la policía usar esta tecnología durante una protesta?

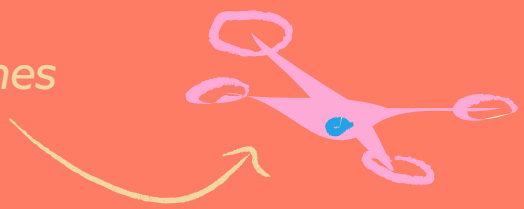
Los agentes de la policía que acompañan las manifestaciones pueden portar body cams y las imágenes capturadas pueden ser procesadas con tecnología de reconocimiento facial.

La policía colombiana usa body cams en Nariño, Antioquia, Santander, Boyacá y Cundinamarca, según el Conpes 4064 de 2021. En junio de 2021, tras las múltiples denuncias por excesos en el uso de la fuerza durante manifestaciones, la policía anunció que comprará más de 11 mil body cams.

¿Esto afecta tus derechos?

El uso de body cams no debería afectar los derechos de los y las manifestantes porque su finalidad es fiscalizar el actuar de la policía. Su uso debe estar restringido a ese propósito y no a vigilar la protesta.

» *Drones*



¿Qué es?

Son vehículos aéreos no tripulados controlados a distancia. Suelen venir equipados con cámaras y podrían estar habilitados con tecnología de reconocimiento facial, altavoces, equipos de vigilancia, radares y herramientas de interceptación de comunicaciones, como los IMSI catchers.

¿Cómo puede la policía usar los drones durante una protesta?

Los drones con cámara pueden utilizarse para vigilar y seguir a distancia los movimientos de los y las manifestantes. Cuando están equipados con tecnologías para interceptar comunicaciones, pueden utilizarse para vigilar y rastrear sus llamadas. Los drones equipados con altavoces pueden usarse para darles órdenes, instrucciones o advertencias a quienes protestan.

En Colombia la policía adquirió drones en 2019, pero no tenemos certeza de sus características técnicas ni de sus usos en el contexto de la protesta.

¿Esto afecta tus derechos?

El impacto en los derechos humanos por el uso de drones para vigilar la protesta no está claro. Si los drones únicamente incorporan cámaras de video, no parece haber diferencias con las cámaras de vigilancia que están instaladas en las ciudades. Si incorporan otras tecnologías como reconocimiento facial o IMSI catchers, suponen un riesgo a la privacidad y a la posibilidad de manifestarse anónimamente.

2. Consejos para proteger tu privacidad durante la protesta

Evita publicar en las redes sociales imágenes en las que aparezcan los rostros de otros/as manifestantes.

Considera usar tapabocas, gorros, pintura facial, máscaras, etc. para dificultar que te identifiquen.

Considera usar herramientas de difuminación de rostros antes de publicar fotos o videos de manifestantes en redes sociales.

IV TUS REDES SOCIALES

1.
¿Cómo puede la policía monitorear tus redes sociales durante una protesta?

La policía usa una estrategia llamada ciberpatrullaje para monitorear el uso de redes sociales durante una protesta.

¿Qué es el ciberpatrullaje?

Es una estrategia de las autoridades para vigilar las comunicaciones de la ciudadanía en Internet.

Durante el paro nacional de 2021, el ciberpatrullaje pudo implicar al menos tres actividades: identificar posibles delitos cometidos en Internet, identificar noticias falsas en redes sociales y realizar perfilamientos a activistas o periodistas críticos con el Gobierno. El ciberpatrullaje se realiza de forma manual por agentes de policía y, según MinDefensa, puede desembocar en procesos judiciales.

La Resolución 05839 de 2015 habilita a la policía para hacer "ciberpatrullaje en la web 24/7". Sin embargo no se han establecido definiciones, límites o procedimientos legales a esta actividad.

2. ¿Cómo afecta tus derechos?

El perfilamiento es una práctica ilegal porque vulnera los derechos fundamentales a la intimidad, a la libertad de expresión y a la protección de datos personales.

3. Consejos para protegerte en redes sociales durante una protesta

- Evita publicar en redes sociales información personal o información que permita tu identificación y la de otras personas que participan de la protesta.
- Si vas a publicar contenido relacionado con la protesta en redes sociales, te recomendamos hacerlo desde cuentas anónimas que no revelen tu identidad.
- Coordina las actividades relacionadas con la protesta (rutas, participantes o puntos de encuentro) a través de grupos de Signal o Whatsapp en los que conozcas la identidad de todos los integrantes.

V CONOCE MÁS EN

Kit de seguridad digital para antes, durante y después de una protesta - Fundación Karisma

Guía de defensa personal contra la vigilancia - Electronic Frontier Foundation (EFF)

Guía práctica de bolsillo para salir a protestar - Dejusticia

Manual de autoprotección contra el Esmad - 070

Recomendaciones para el cubrimiento de manifestaciones sociales - Fundación para la Libertad de Prensa (FLIP)

Dejusticia

Fundación Karisma