Guía de Protesta

por los Derechos Civiles

Asociación por los Derechos Civiles

Noviembre 2021
adc.org.ar

Redacción: Alejo Kiguel
Diagramación: Matías Chamorro
Diseño de tapa: El Maizal

Contenido

La *Guía de Protesta* es una campaña que intenta concientizar sobre las herramientas tecnológicas que las fuerzas de seguridad podrían utilizar para monitorear e identificar personas en una protesta.

La ADC viene haciendo un seguimiento continuo sobre la compra y utilización de tecnologías de vigilancia en Argentina. En años anteriores realizamos investigaciones para conocer los riesgos de la utilización de drones por parte de las fuerzas de seguridad,[1] nos pronunciamos sobre la utilización del ciberpatrullaje[2] y trabajamos activamente para detener la utilización de tecnologías de reconocimiento facial en espacios públicos. Sobre la utilización de reconocimiento facial, lanzamos la web conmicarano.org.ar donde evidenciamos en un mapa las provincias y municipios de nuestro país en donde esta tecnología ya está siendo utilizada. Por otro lado, en el 2021 en conjunto con otras organizaciones de la sociedad civil de Latinoamérica realizamos una investigación conjunta para conocer quiénes son las empresas que desarrollan y venden estas tecnologías a los estados.[3]

Aunque en Argentina aún resulta incipiente la utilización de estas tecnologías en protestas y manifestaciones, la creciente compra de tecnologías de vigilancia por parte del Estado como cámaras de seguridad, tecnologías de reconocimiento facial, herramientas de extracción forense de dispositivos electrónicos, drones, y la utilización del ciberpatrullaje evidencian un claro avance de este tipo de prácticas, que constituyen un peligroso avance para los DD.HH.

En esta ocasión nos queremos concentrar en explicar cómo las personas pueden intentar evitar ser víctimas de este tipo de tecnologías de vigilancia. A continuación, detallamos cómo las mismas están siendo utilizadas en el mundo para vigilar las protestas, y también brindamos una serie de recomendaciones para protegerte de esta vigilancia.

1. Vigilancia de tus dispositivos electrónicos

a) Imágenes, contactos, documentos y otra información de tu teléfono

¿Dónde se almacenan mis imágenes, documentos y contactos?

- **Cada vez que usas tu teléfono estás generando datos. Por ejemplo, cuando sacas fotos o grabás vídeos, cuando creás o editás notas y documentos, y cuando agregás nuevos nombres y números a tu agenda de contactos.**

- **Es importante tener en cuenta que cuando creás un archivo en tu teléfono, la mayoría de las veces también generás ‘’información asociada’’ o “metadatos” (por ejemplo, cuando sacás una foto se pueden generar metadatos como la hora y el lugar en que se tomó). Estos metadatos pueden ser tan reveladores, si no más, que la propia foto.**

- **Todos estos datos quedan guardados en la memoria interna de tu teléfono (incluyendo cualquier memoria externa conectada, como una tarjeta MicroSD), o en la nube, o en ambas si estás usando algún servicio en la nube como copia de seguridad.**

¿Cómo puede acceder la policía a la información de mi teléfono?

- **Hay algunas formas en las que la policía podría acceder a estos datos, dependiendo de cómo estén almacenados:**

- Si almacenás tus datos localmente en tu teléfono, entonces es posible acceder a ellos mediante **herramientas de extracción forense de dispositivos móviles,** que se conecta a tu teléfono y descarga todos los datos almacenados en él. Este método no puede utilizarse a distancia: la policía debe tener acceso físico a tu teléfono.

- Si sincronizás tus imágenes, documentos y contactos utilizando algún servicio en la nube (iCloud, Dropbox o Google Drive, por ejemplo), la policía podría utilizar **herramientas de "extracción en la nube"** para acceder a esta información, o puede hacer un requerimiento legal al proveedor el servicio en la nube.

Herramientas de extracción forense de dispositivos móviles

¿Qué hacen las herramientas de extracción forense de teléfonos móviles?

- **Las herramientas de extracción forense de dispositivos móviles (EFDP) son dispositivos que permiten extraer datos e información de los teléfonos celulares, incluyendo:**
  - contactos;
  - datos de llamadas (es decir, información sobre a quién llamaste o te llamó, cuándo y durante cuánto tiempo);
  - mensajes de texto (incluyendo a quién se envió mensajes de texto y cuándo);
  - archivos almacenados (fotos, vídeos, archivos de audio, documentos, etc.);
  - datos de aplicaciones (incluidos los datos almacenados en estas aplicaciones);
  - historial de localización;

- historial de búsqueda en tus navegadores
- conexiones a redes wifi (que pueden revelar las ubicaciones de cualquier lugar donde te hayas conectado a wifi, como tu lugar de trabajo o una cafetería).

¿Cómo podrían utilizarse las herramientas de extracción de teléfonos móviles en una protesta?

- **Para extraer los datos almacenados, la policía tendría que acceder físicamente a tu teléfono.**

- **En un contexto de protesta o manifestación, la policía podría detenerte o demorarte si existen indicios de que hayas cometido un delito. En estos casos la policía debe informar inmediatamente al juez desde el lugar, quien podría ordenar que te detengan y retengan tus pertenencias como es el teléfono celular.**

- **En algunos casos, la policía también podría llevarse tu teléfono si fuiste testigo o incluso víctima de un delito.**

- **En Argentina, la mayoría de las fuerzas policiales cuentan con estas herramientas de extracción y análisis de dispositivos móviles. Sin embargo, para poder utilizarlas necesitan de una orden judicial para poder revisarlo.**

Recomendaciones para proteger la información de tu celular. Lo que hay que tener en cuenta:

- **Como usuario del dispositivo, tenés cierto control sobre los datos que generás y dónde se almacenan. Tener un buen conocimiento de la información que tu teléfono tiene**

significa que en caso de que accedan a tu teléfono, al menos vas a saber a qué datos están accediendo.

- **Mantener el sistema operativo de tu teléfono (Android o iOS) actualizado es probablemente la mejor manera de prevenir que puedan acceder a tu celular a través de una de estas herramientas.**

- **Aunque deberías mantener tu teléfono bloqueado, algunas herramientas de extracción forense de celulares están diseñadas para acceder incluso a teléfonos bloqueados. Sin embargo, tener el sistema operativo actualizado y una contraseña de acceso robusta debe ser tu primera medida de protección.**

- **Antes de ir a una protesta, podés considerar la posibilidad de hacer una copia de seguridad de los datos de tu teléfono en tu computadora, y luego eliminar esos datos de tu teléfono. Tené en cuenta que algunas herramientas de extracción forense de dispositivos móviles pueden recuperar los datos borrados. Si guardaste los datos en un servicio en la nube, algunas herramientas de extracción forense de dispositivos móviles pueden seguir accediendo a esos datos.**

Herramientas de “extracción de nube”

¿Qué son las “herramientas de extracción de nube” y para qué sirven?

- **La tecnología de extracción en la nube permite acceder a los datos almacenados en tu “nube” a través de tu celular u otros dispositivos.**

- **El uso de herramientas de extracción en la nube permite acceder a los datos que almacenás en línea. Algunos ejemplos de aplicaciones que almacenan datos en la nube son Instagram, Telegram, Twitter, Facebook y Uber.**

¿Cómo se pueden utilizar las herramientas de extracción de nube en una protesta?

- **Para extraer tus datos de la nube, la policía tendría que acceder físicamente a tu teléfono. La policía podría confiscar tu teléfono si te detuvieron durante una protesta, pero también si fuiste testigo o incluso víctima de un delito.**

- **Toda esta información podría utilizarse para identificar a los manifestantes y organizadores y conocer la ubicación de las protestas y acciones.**

- **Tus datos en la nube no solo revelan tu información, también pueden revelar mucho sobre tus amigos, familia y cualquier otra persona con la que interactúes en línea. Por ejemplo, puede ser que tengas viejos contactos almacenados en la nube, que han sido borrados del propio teléfono.**

Para tener en cuenta al ir a una protesta:

- **Una posibilidad es desactivar la copia de seguridad en la nube en las aplicaciones del teléfono que usas, y cerrar sesión en todos los servicios basados en la nube. Esto evitará que los datos se almacenen en la nube y va a impedir el acceso a estos datos desde tu teléfono móvil.**

- **Antes de acudir a una protesta, tené en cuenta que, aunque utilices comunicaciones cifradas de extremo a extremo a través de WhatsApp, si haces una copia de seguridad de tus mensajes de WhatsApp en la nube, la policía podría acceder a estas copias de seguridad cifradas utilizando herramientas de extracción en la nube en tu teléfono.**

- **Algunas aplicaciones, como Uber, Twitter, WhatsApp y Facebook te permiten desactivar los datos de localización que se almacenan en la Nube. Esto puede evitar que la policía pueda rastrear dónde estuviste.**

- **Como usuario del dispositivo, tenés cierto control sobre los datos que generas en primer lugar, y dónde se almacenan. Tener un buen conocimiento de la información que guarda tu teléfono significa que, en caso de que accedan a tu teléfono, al menos vas a saber a qué datos están accediendo.**

b) “Identificadores únicos” de tu teléfono

¿Qué son mis “identificadores únicos” y dónde se almacenan?

- **Tu teléfono y tu tarjeta SIM contienen identificadores únicos, a los que la policía puede acceder para identificarte.**

- **El IMSI (International Mobile Subscriber Identity) es un número único asociado a tu tarjeta SIM. No cambia, aunque pongas la tarjeta SIM en un teléfono diferente.**

- **En Argentina, todos los dueños de líneas de telefonía celular deben registrar sus datos en los registros de las compañías de telefonía celular, por lo que si tenés una suscripción,**

seguramente el IMSI esté asociado a información personal como tu nombre y dirección.

- **El IMEI (International Mobile Equipment Identity) es un número único que identifica tu teléfono (el dispositivo). Por lo tanto, si cambias de teléfono, tendrás un nuevo IMEI.**

- **El IMSI y el IMEI no pueden ser alterados de otra manera, y pueden estar vinculados a información sobre tu persona (por ejemplo, nombre, dirección) o tu dispositivo (por ejemplo, marca, modelo).**

- **Otros identificadores: Hay algunos otros componentes en tu teléfono con identificadores únicos, como la dirección MAC de tu antena wifi, la BD_ADDR de tu módulo Bluetooth o el identificador de publicidad.**

¿Cómo puede acceder la policía a mis identificadores únicos?

- **Las aplicaciones y los sitios web de tu teléfono pueden acceder a tu identificador publicitario. Aunque no está directamente asociado a tu información personal (por ejemplo, tu nombre y dirección), puede estar asociado a otros datos como tu ubicación. Algunos corredores de datos[4] obtienen cantidades masivas de datos de los teléfonos y los venden a la policía, incluyendo identificadores de publicidad.**

- **Otros identificadores únicos, como tu dirección MAC, pueden ser recogido cuando te conectás a una red de wifi, pero es mucho más difícil asociarlos con información personal que pueda ser utilizada para identificarte.**

- **Además, la policía también podría conocer los identificadores asociados a tu persona a través de consultas a las compañías de telefonía móvil.**

- **La policía también podría intentar obtener tu IMSI e IMEI con un receptor IMSI (IMSI Catcher), un dispositivo desplegado para rastrear todos los teléfonos conectados a la red en sus proximidades. Una vez interceptado este identificador, podría utilizarse para obtener otra información personal.**

¿Qué es un receptor IMSI (IMSI Catcher)?

- **IMSI", por sus siglas en inglés, es la clave de servicio del suscriptor y consiste en un número único para tu tarjeta SIM. Los receptores IMSI (IMSI Catcher) también se conocen como Stingrays.**

- **Un receptor IMSI es un dispositivo que localiza y rastrea todos los teléfonos que están conectados a una red telefónica en su proximidad, "capturando" el número IMSI único.**

- **Lo hace simulando ser una torre de telefonía móvil, engañando a los teléfonos celulares cercanos para que se conecten a ella, lo que le permite interceptar los datos de ese teléfono comunicados a esa torre de telefonía sin que el usuario del teléfono lo sepa.**

- **La información que pueden conseguir con esta herramienta es tu ubicación aproximada. Es inevitable que las torres de telefonía conozcan tu ubicación aproximada a través de la triangulación; de hecho, así es como te proporcionan su**

servicio en primer lugar. Al interponerse entre tu celular y la torre de telefonía, un receptor IMSI puede averiguar tu ubicación aproximada.

- **Dependiendo de las capacidades del receptor IMSI y de la red a la que se conecte tu teléfono, podrían producirse ataques más avanzados, aunque es poco probable. Algunos dispositivos Stingray se basan en debilidades conocidas de los protocolos de comunicación y pueden forzar a tu teléfono a degradar los protocolos que está utilizando, para hacer que tus comunicaciones sean menos seguras y más fácilmente accesibles (por ejemplo, degradando las comunicaciones de 3G a 2G, ya que, por lo que sabemos, la interceptación de contenidos y el descifrado en tiempo real sólo pueden realizarse cuando el objetivo está conectado a través de la red 2G).**

- **Los receptores IMSI no pueden leer el contenido de los mensajes encriptados que intercambiás a través de plataformas que utilizan el cifrado de extremo a extremo (por ejemplo, WhatsApp o Signal).**

¿Cómo podrían utilizarse los receptores IMSI en una protesta?

- **La policía podría utilizar los receptores IMSI para identificar quién estuvo en una protesta, capturando los números IMSI de todos los teléfonos que estuvieron en proximidad a esa protesta, lo cual entraría en claro conflicto con los derechos a la libertad de expresión, de reunión y asociación, y a la privacidad.**

- **Algunos tipos de receptores IMSI pueden incluso bloquear tus llamadas y mensajes.**

Para tener en cuenta al ir a una protesta:

- **Poner tu teléfono en modo avión o apagarlo por completo hará que un receptor IMSI no pueda rastrearte a vos ni a tus comunicaciones.**

- **Si querés evitar que el contenido de tus mensajes de texto sea rastreado por un receptor IMSI, podés utilizar servicios de mensajería que utilizan el cifrado de extremo a extremo, como Signal y WhatsApp. La única información que un receptor IMSI podría recoger es el hecho de que estás usando estas aplicaciones, pero no el contenido en sí.**

- **Utilizar un bloqueador de anuncios también es una buena forma de evitar que las empresas te rastreen en línea y recopilen tu información personal.**

c) Localización a través de tu teléfono celular

¿Dónde se almacenan los datos de localización de mi teléfono?

Tu teléfono puede ser localizado de dos maneras principales, utilizando el GPS o la localización de la red móvil:

1. GPS

- **El GPS (Sistema de Posicionamiento Global) utiliza la navegación por satélite para localizar tu teléfono con**

bastante precisión (dentro de unos pocos metros), y se basa en un chip GPS dentro de tu teléfono.

- **Dependiendo del teléfono que uses, los datos de localización GPS pueden almacenarse localmente y/o en un servicio en la nube como Google Cloud o iCloud. También podrían ser recogidos por cualquier app que utilices y que tenga acceso a tu ubicación GPS.**

2. Ubicación de la red móvil

- **La localización de la red móvil (o localización del Sistema Global de Comunicaciones Móviles [GSM]) depende de tu red celular y puede determinarse solo por estar conectado a la red (es decir, tu teléfono está encendido y no en modo avión), pero es mucho menos precisa que el GPS. Tu ubicación aproximada puede determinarse con un rango de precisión de unas decenas de metros en una ciudad, o de cientos de metros en zonas rurales.**

- **Estos datos de localización son almacenados por tu proveedor de red.**

También se podrían utilizar otros métodos para determinar tu ubicación de forma indirecta, como los puntos de acceso wifi abiertos y las balizas Bluetooth a las que se conecta tu teléfono o los metadatos de ubicación incrustados en tus fotos.

¿Cómo acceder a mis datos de localización?

Hay una serie de métodos que la policía podría utilizar para acceder a tu ubicación (del teléfono):

1. GPS

- **El acceso a los datos de localización del GPS depende de dónde se almacenen los datos. Puede hacerse mediante un dispositivo de "extracción de teléfonos móviles", que se conecta a tu teléfono y descarga todos los datos almacenados en él, incluidos los detalles de los lugares que visitaste. Este método requiere que la policía acceda físicamente a tu teléfono.**

- **El acceso a los datos de tu GPS también puede ser posible a través del hackeo de tu dispositivo, una técnica avanzada que podría no requerir necesariamente el acceso físico a tu teléfono y podría hacerse de forma remota.**

- **Si tus datos GPS también están almacenados en una cuenta online (por ejemplo, iCloud o Google Maps), se puede acceder a ellos a través de tecnologías de extracción en la nube o de solicitudes legales a las empresas que almacenan esos datos.**

2. Localización de la red móvil

- **La policía puede acceder a tus datos de localización aproximados a través de tu proveedor de servicios. En Argentina se exige una orden judicial para solicitar esta información.**

- **Esto significa que la policía no necesita acceder a tu teléfono para determinar que estuviste a cierta distancia de una protesta.**

- **Otra forma de acceder a esta misma información es utilizar un receptor IMSI (también conocido como Stingray), un dispositivo desplegado para interceptar y rastrear todos los teléfonos celulares encendidos y conectados a una red móvil en una zona específica. Simulando ser una torre de celular, permite extraer información de ciudadanos en protestas, reuniones o eventos públicos, con el fin de obtener información acerca de las personas que asisten.**

Cómo controlar mejor tus datos de localización

1. GPS

- **La mejor manera de evitar que puedan acceder a tu ubicación es limitar la generación de los datos de localización en primer lugar.**

- **En el caso del GPS, para hacerlo deberías apagar tu GPS (a menudo denominado "servicios de localización"). Sin embargo, aunque lo apagues, los datos de localización de cualquier ocasión anterior en la que lo tuvieras activado podrían seguir siendo accesibles.**

- **Si todavía necesitás usar el GPS en tu teléfono, revisá los permisos de las aplicaciones individuales para acceder a tu ubicación.**

- **Eliminar los permisos de acceso a tu ubicación para todas las aplicaciones puede evitar que estos datos se almacenen en una cuenta online.**

- **Si es absolutamente necesario que una aplicación tenga acceso a tus datos GPS, inspeccioná la configuración de esa**

aplicación para asegurarte de que entendés si tu ubicación se almacena en línea o sólo localmente en tu aplicación. Por ejemplo, si utilizas Google Maps mientras estás conectado a una cuenta de Google, es posible que quieras desactivar el historial de ubicaciones en la configuración para que no se almacene en tu cuenta de Google.

- **Si tomaste fotos con los servicios de ubicación activados, la ubicación donde se tomó la foto podría incluirse en los metadatos (conocidos como datos EXIF) de la imagen. Es posible que quieras desactivar los servicios de localización mientras tomas las fotos, o puedes usar un software o una app para borrar estos datos EXIF después (por ejemplo, la app de mensajería Signal borra los datos EXIF cuando envías imágenes).**

- **Del mismo modo, apagar el wifi o el Bluetooth puede evitar que tu teléfono se conecte a puntos de acceso no deseados y proporcione información de ubicación indirecta.**

2. Red móvil

- **Cuando se trata de la localización de la red móvil, la única manera de tener control sobre ella es evitar la conexión a la red en absoluto.**

- **Tener el teléfono apagado, en modo avión o en una jaula de Faraday[5] va a impedir la conexión a la red móvil y, por tanto, hará imposible la geolocalización GSM. Una jaula de Faraday o apagar el teléfono impide cualquier tipo de conexión a cualquier red telefónica. En cambio, si sólo utilizas el modo avión podrás seguir realizando algunos tipos de conexión (por ejemplo, Bluetooth o GPS).**

d) Monitoreo de redes sociales

¿Qué es el monitoreo de redes sociales?

- **El monitoreo de las redes sociales o ciberpatrullaje se refiere al seguimiento, la recopilación y el análisis de la información compartida en las plataformas de las redes sociales, como Facebook, Twitter, Instagram.**

- **Puede incluir el monitoreo de contenidos publicados en grupos o páginas públicas o privadas. También puede implicar el scraping, es decir, la obtención de todos los datos de una plataforma de medios sociales, incluido el contenido que publicas y datos sobre tu comportamiento (como lo que te gusta y compartís).**

- **El monitoreo de las redes sociales permite recoger y analizar una gran cantidad de datos, que pueden utilizarse para generar perfiles y predicciones sobre los usuarios.**

- **En Argentina la regulación legal del monitoreo de redes sociales -o ciberpatrullaje- es poco clara. Aunque existieron intentos de regular estas prácticas a través de resoluciones ministeriales y protocolos, desde la ADC sostenemos que en tanto no exista un sustento legal proveniente del órgano legislativo, estos no pueden considerarse constitucionales.**[6]

¿Cómo se podría utilizar el monitoreo de las redes sociales en relación con las protestas?

- **Los organizadores de las protestas suelen utilizar las redes sociales para organizarlas, comunicarse con los manifestantes y subir fotos y vídeos.**

- **Esto significa que la policía podría recopilar datos de las páginas y grupos en redes sociales para conocer las identidades y afiliaciones de los organizadores, la ubicación y el momento de la acción planificada, y otra información relacionada.**

- **La policía podría rastrear publicaciones en redes sociales relacionadas con protestas pasadas o futuras para identificar a los manifestantes.**

- **La policía también podría aplicar tecnología de reconocimiento facial a las imágenes y vídeos de las protestas subidos a las redes sociales para identificar a los manifestantes.**

Para tener en cuenta al ir a una protesta

- **Si subís tus imágenes de la protesta a tus redes sociales, podrían ser utilizadas para identificar y ubicar a las personas en el lugar de la protesta.**

- **Si la configuración de la ubicación está activada en tus plataformas de redes sociales o en tus aplicaciones de cámara y fotografía, y luego publicás cerca del lugar de una protesta, la policía podría tener acceso a esos datos de ubicación.**

- **Si querés utilizar las redes sociales mientras estás en una protesta, deberías considerar la posibilidad de desactivar los ajustes de localización en aplicaciones que vayas a utilizar. Si compartís imágenes de la protesta, no etiquetes a personas que hayan participado en ella sin su consentimiento, ya que esto podría crear un rastro en el que**

la policía podría basarse para ubicar a las personas en la protesta.

- **Si subís fotos de la protesta a las redes sociales, considerá eliminar los datos EXIF de antemano. Los datos EXIF son metadatos asociados a tus imágenes que pueden revelar información como la ubicación, la hora y la fecha y el dispositivo utilizado.**

- **Tené cuidado: las imágenes pueden seguir siendo geolocalizadas a partir de información de fondo (por ejemplo, un monumento o punto de referencia). Consideralo al filmar tu entorno y tratá de evitar los fondos identificables.**

2. Una guía sobre la vigilancia de tu rostro y tu cuerpo

a) Reconocimiento facial

¿Qué es la tecnología de reconocimiento facial?

- **La tecnología de reconocimiento facial (TRF) es una tecnología biométrica que permite reconocer e identificar a las personas mediante los rasgos de su rostro.**

¿Cómo funciona?

- El reconocimiento facial funciona mediante un software alimentado por un algoritmo (una fórmula) que está entrenado para reconocer rostros e individualizar sus rasgos.

- Una vez que se realiza el mapeo de los rasgos faciales, el software genera una plantilla con la representación matemática para ese rostro único. Esa plantilla es el dato biométrico dentro de la tecnología de reconocimiento facial.

- Con la plantilla biométrica el rostro ya puede ser leído por una computadora y contrastado con una base de datos que previamente almacenó todo un conjunto de rostros.

- El software puede llevar a cabo una comparación en tiempo real con todos los rostros almacenados en esa base de datos para determinar si una persona se encuentra registrada allí.

- La biometría es un proceso de probabilidades, por lo que una vez que el software encuentra una potencial coincidencia, arroja un porcentaje que define qué tan probable es que corresponda a la misma persona.

- En Argentina, cada vez más lugares implementan estos sistemas sin haber realizado evaluaciones de impacto en derechos humanos. En el micrositio https://conmicarano.adc.org.ar/ recopilamos las distintas iniciativas de reconocimiento facial que se están desplegando en Argentina.[7]

¿Cómo podría utilizarse en una protesta?

- **El Reconocimiento Facial podría utilizarse para vigilar, rastrear e identificar los rostros de las personas en espacios públicos, incluso en protestas. Esto puede hacerse abierta o furtivamente, sin que las personas lo sepan o lo consientan.**

- **Las cámaras con tecnología de RF pueden tomar fotos o vídeos e identificar a las personas en tiempo real o en un momento posterior. También puede utilizarse para analizar e identificar imágenes existentes, por ejemplo, fotos y vídeos subidos a las redes sociales.**

- **A medida que se recogen los datos biométricos de los manifestantes, estos pueden añadirse a una o más bases de datos preexistentes, donde pueden compararse con los datos biométricos de otras fuentes para encontrar una coincidencia.**

- **Estos datos también podrían utilizarse para crear una nueva base de datos de las personas que asisten a las protestas, con el fin de realizar futuras comparaciones e identificaciones.**

Para tener en cuenta cuando vas a una protesta:

- **El RF funciona a partir de la captación de la cara de una persona, así que si querés intentar mantener el anonimato, podés considerar la posibilidad de llevar la cara cubierta, por ejemplo, con un pañuelo.**

- **Otras opciones para interrumpir el RF incluyen el uso de pintura y ropa con diseños destinados a interferir con el reconocimiento facial preciso. Sin embargo, el RF se adapta y mejora constantemente, por lo que las pinturas faciales y estos otros métodos pueden resultar menos eficaces en el futuro.**

- **La tecnología de RF también puede ser utilizada en las redes sociales. Tené esto en cuenta antes de publicar cualquier imagen de una protesta en la que aparezcan los rostros de otros manifestantes.**

- **Otra opción es utilizar herramientas de difuminación de rostros antes de publicar fotos o vídeos en línea.**

b) Cómo se pueden utilizar las cámaras corporales en una protesta

¿Qué hacen las cámaras de vídeo corporales?

- **Las cámaras corporales son cámaras de videograbación que se fijan a la ropa de un agente de policía -a menudo a la altura del pecho, los hombros o la cabeza- y pueden grabar vídeo, incluido el sonido, desde la perspectiva del agente.**

- **Las cámaras corporales probablemente las puedas ver en el pecho de la policía, y cuando estén grabando, debería aparecer una luz intermitente en el dispositivo.**

- **En Argentina, son utilizadas por la mayoría de las fuerzas de seguridad.**[8]

¿Cómo podrían utilizarse las cámaras de video corporales en una protesta?

- **Las cámaras corporales pueden utilizarse en las protestas para controlar las acciones de los manifestantes.**

- **Fuera del contexto de las protestas, las cámaras corporales normalmente se encienden sólo al comienzo de un incidente. Pero en una protesta, pueden permanecer encendidas durante todo el tiempo.**

- **Algunas cámaras exigen que el vídeo se cargue manualmente en un servidor, pero algunas de las cámaras de videovigilancia más recientes permiten que las imágenes se transmitan en directo a una comisaría.**

- **Aunque en Argentina no tenemos información de que se utilicen con este fin, la grabación podría ser procesada posteriormente, por ejemplo, mediante un software de reconocimiento facial.**

Para tener en cuenta al acudir a una protesta:

- **Aunque la policía suele afirmar que las cámaras corporales actúan como "testigos independientes" que disuaden**

el abuso policial, lo cierto es que los agentes de policía pueden encender y apagar las cámaras o decidir hacia dónde dirigirlas, por lo que tienen el control de lo que graban, y de lo que no graban.

- Véase nuestra guía separada sobre la tecnología de reconocimiento facial, relativa al procesamiento de las grabaciones de las cámaras corporales por el software de reconocimiento facial.

c) Cómo se pueden utilizar drones policiales en una protesta

¿Qué son los drones policiales?

- Los drones son vehículos aéreos no tripulados (VANT) controlados a distancia y de distintos tamaños.

- Suelen venir equipados con cámaras y eventualmente podrían estar habilitados con otras herramientas más sofisticadas, como tecnología de reconocimiento facial, lectores de patentes de vehículos terrestres, o determinación de ubicación geográfica por GPS, entre otros.[9]

- Los drones también pueden estar equipados con altavoces, equipos de vigilancia, radares y herramientas de interceptación de comunicaciones, como los receptores IMSI.

¿Cómo podrían utilizarse los drones durante las protestas?

- Los drones con cámara pueden utilizarse para vigilar y seguir a distancia los movimientos de las personas en

espacios públicos, incluso en protestas, sin que éstas den su consentimiento o lo sepan.

- **Del mismo modo, cuando están equipados con tecnologías de interceptación de comunicaciones, los drones pueden utilizarse para vigilar y rastrear las llamadas y los mensajes de los manifestantes, en la zona en la que se desarrolla una protesta y en sus alrededores**

Para tener en cuenta cuando vas a una protesta:

- **El uso de drones y el impacto en tu anonimato depende de las tecnologías con las que estén equipados.**

- **Consultá nuestras guías sobre la tecnología de reconocimiento facial y los receptores IMSI, ya que son herramientas que un dron podría utilizar para vigilar las actividades de los manifestantes.**

* * *

3. Notas

1 https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf

2 https://adc.org.ar/2020/04/22/sobre-la-necesidad-de-una-ley-para-regular-la-investigacion-en-fuentes-abiertas-y-redes-sociales/

3 El informe completo se encuentra disponible en https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/

4 Los corredores de datos son empresas que se dedican a comprar y vender la información que generás a través del uso de internet. Mas información en https://www.amnesty.org/es/latest/research/2017/02/muslim-registries-big-data-and-human-rights/

5 Una jaula o bolsa de Faraday es un producto que frena la propagación de señales electromagnéticas e inhibe cualquier señal a tu teléfono o equipo informático. Una forma casera de generar una jaula de faraday es envolviendo tu equipo con grandes cantidades de papel aluminio. Así, se inhibirán todas las señales.

6 Para conocer más sobre el ciberpatrullaje en Argentina, conocé visitá nuestra web https://adc.org.ar/2020/04/22/sobre-la-necesidad-de-una-ley-para-regular-la-investigacion-en-fuentes-abiertas-y-redes-sociales/

7 Con Mi Cara No. https://conmicarano.adc.org.ar/, un micrositio de la ADC exclusivamente dedicado a brindar información sobre reconocimiento facial y alertar a la población sobre los peligros de esta tecnología

8 https://www.argentina.gob.ar/noticias/frederic-entrego-400-camaras-de-video-de-montaje-corporal-para-las-fuerzas-federales

9 Más información sobre el uso de drones en argentina disponible en https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf


APC
por los Derechos Civiles