MANIFESTACIONES LIBRES

Guía sobre la vigilancia policial en manifestaciones en Paraguay

TEDIC
TECNOLOGÍA & COMUNIDAD

MANIFESTACIONES LIBRES

Guía sobre la vigilancia policial en manifestaciones en Paraguay

TEDIC
TECNOLOGÍA & COMUNIDAD

TEDIC
TECNOLOGÍA &
COMUNIDAD

TEDIC es una organización sin fines de lucro, fundada en el 2012 que defiende y promueve los derechos humanos en entornos digitales, con foco en desigualdades de género y sus intersecciones en Paraguay y la región de América Latina.

Privacy International (PI) es una ONG de Reino Unido, formada en 1990, que busca proteger la privacidad por parte de gobiernos y corporaciones en el mundo.

Elaboración: Maricarmen Sequera

Coordinación: Eduardo Carrillo

Corrección de estilo: Luis Alonzo Fulchi

Diagramación: Horacio Oteiza

Diseño e ilustración: Enrique Bernardou

ASUNCIÓN · PARAGUAY · MARZO 2022

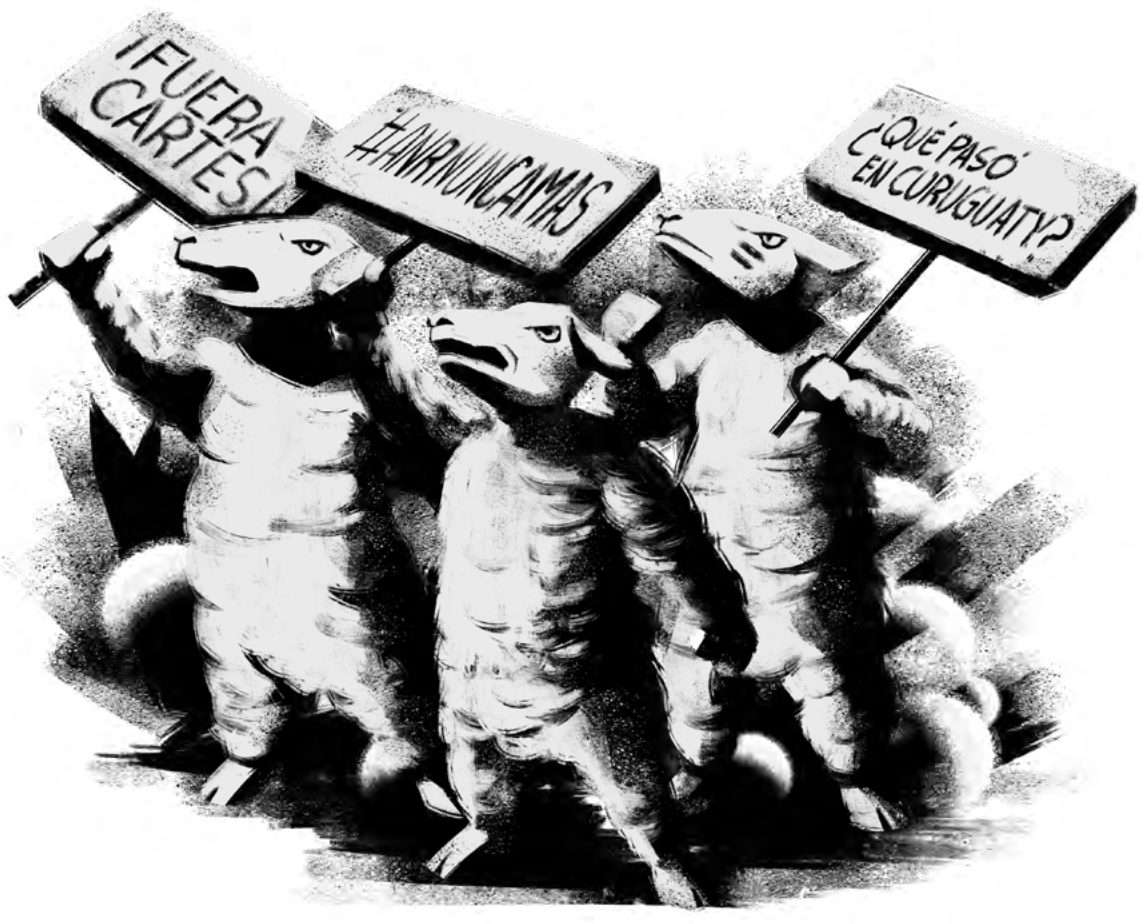
Contenido

Resumen

En las democracias liberales contemporáneas, las libertades de reunión y asociación son derechos fundamentales y garantizan que cada ciudadano pueda reunirse en grupos, manifestaciones, partidos, sindicatos o unirse para un propósito particular. Internet trae nuevos contornos a estas libertades.

La protesta o manifestación pública es un derecho fundamental y no debe ser criminalizada. Las calles son espacios de disputa y su vigilancia se vuelve más sofisticada por el uso de tecnología por parte de las fuerzas de seguridad (Cámaras de reconocimiento facial, IMSI catcher, vigilancia en redes sociales etc). La presencia de la Policía Nacional paraguaya y las fuerzas del sistema de seguridad y justicia, debería estar orientada a garantizar que pueda ejercerse este derecho de manera pacífica. Sin embargo, generalmente, es criminalizada, poniendo en riesgo el ejercicio de los derechos fundamentales de la ciudadanía.

Esta guía ofrece una serie de propuestas sobre cómo las personas que se manifiestan de forma pacífica deben protegerse durante un evento público.



VIGILANCIA POLICIAL DE TUS DISPOSITIVOS

¿Dónde se almacena tu información?

- Cada vez que usas cualquier dispositivo (computadora, teléfono, tablet, etc.) estás generando información. Por ejemplo, cuando tomás 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 dispositivo, la mayoría de las veces también generás «información asociada» o «metadatos» (por ejemplo, cuando tomás 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.
- La información a la que accedería la policía no sólo se referirá a vos, sino que contendrá datos personales, como mensajes o fotos, relacionados con familiares, amigos y colegas. La policía puede almacenar todos estos datos de forma indefinida y combinarlos con otros datos que posee para construir una imagen aún más invasiva a nuestras vidas.
- 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. Pueden incluir datos basados en aplicaciones, incluidos los de plataformas populares como Facebook, Google, Twitter, TikTok, Instagram y otras.
- Las comunicaciones tradicionales de los teléfonos móviles se realizan a través de la red celular. Sueles acceder a ellas con las aplicaciones de mensajes de texto y llamadas telefónicas que vienen preinstaladas tu teléfono. Los registros de llamadas telefónica (metadatos) y los mensajes de textos se almacenan en tu dispositivo localmente, en la del destinatario y en la proveedora de Internet de forma temporal[1].

1 En Paraguay. La resolución de CONATEL 1350/2002 que establece un plazo de 6 meses para la conservación del registro de llamadas entrantes y salientes de las telefónicas por parte de las empresas proveedoras de telefonía.

¿Cómo puede acceder la policía a tu información?

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

- Si almacenas todos tus datos localmente en tu teléfono, entonces la policía puede acceder a ellos mediante un dispositivo de «extracción de teléfonos móviles», que se conecta a tu teléfono y descarga todos los datos almacenados en él. Este método no puede utilizarse a distancia: la policía necesita tener acceso físico a tu teléfono.
- El hackeo de dispositivos es una técnica avanzada que permite acceder a cierta cantidad de datos de tu teléfono, pero no necesariamente a todos. A diferencia de la extracción de teléfonos móviles, el hackeo no requiere necesariamente el acceso físico a tu dispositivo. Entonces, este método puede utilizarse en cualquier momento: antes o después de una manifestación.
- Si sincronizas tus imágenes, documentos y contactos utilizando algún servicio en la nube (iCloud, Dropbox o Google Drive, por ejemplo), la policía puede utilizar herramientas de «extracción en la nube» de forma remota para acceder a esta información sin tu autorización o conocimiento, o puede hacer una petición legal al proveedor del servicio en la nube.

¿Cómo limitar el riesgo de que accedan a tu información?

- Para evitar ser objetivo de las técnicas de extracción en la nube, tendrías que abstenerte de utilizar los servicios en la nube por completo.
- Si renunciar por completo a los servicios de la nube resulta demasiado inconveniente, considera no subir contenido sensible a la nube. Revisar la configuración y las funciones de las aplicaciones también es una buena manera de asegurarte de que sabes qué datos de tu teléfono se están respaldando en línea. Un ejemplo de esto son las copias de seguridad de google fotos que se almancenen en el Google Drive. Por otro lado WhatsApp ha actualizado su cifrado para la copia de seguridad[2] de sus mensajes cuando almacena en el Google Drive e iCloud[3] esto nos permite proteger todos nuestros mensajes, notas de audio, fotos, vídeos y archivos a accesos no autorizados. Si aún no actualizaste y configuraste el cifrado extremo a extremo de tu copia de seguridad, se expone a que se pueda acceder utilizando herramientas de extracción en la nube desde la copia de seguridad de Google Drive o iCloud.
- Como persona usuaria del dispositivo también tenés cierto control sobre tu información 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.
- Asegurate que el contenido del teléfono está cifrado y de que el sistema operativo y las aplicaciones están actualizados mitigará algunos métodos de extracción del teléfono móvil y de hackeo del dispositivo.

---

2 FAQ de Whatsapp. How to turn on and turn off end-to-end encrypted backup https://faq.whatsapp.com/general/chats/how-to-turn-on-and-turn-off-end-to-end-encrypted-backup/?lang=en

3 Cómo cifrar tu copia de seguridad de Whatsapp. Actualización 2021. https://www.xatakandroid.com/tutoriales/como-cifrar-tu-copia-seguridad-whatsapp-para-proteger-tus-mensajes-archivos-nube

- Tus mensajes de texto y llamadas telefónicas pueden ser interceptados, grabados e intervenidos por la policía mediante un receptor IMSI, un dispositivo desplegado para rastrear todos los teléfonos móviles encendidos y conectados a la red en una zona específica.
- También se puede acceder a tus mensajes de texto mediante un proceso legal dirigido a tu proveedor de servicios de telefonía e Internet. Se pueden utilizar procesos legales similares para solicitar datos a las empresas que puedan alojar tus comunicaciones (por ejemplo, Facebook).

¿Cómo puede utilizarse la extracción de teléfonos móviles en una manifestación y cómo podés minimizar los riesgos para tus datos?

Extracción de teléfonos móviles

La extracción del teléfono móvil (MPE)[4] permite a la policía acceder y descargar todos los datos almacenados en tu teléfono móvil. Para la mayoría de personas, esto incluirá la información más privada que almacenan en todo su dispositivo, incluyendo sus contactos, mensajes, historial de navegación e información bancaria. Para que suceda esto, primero las fuerzas de seguridad deben sacarte el dispositivo que tenés en tu poder.

Las herramientas de MPE están diseñadas para acceder a teléfonos bloqueados , aunque su capacidad para hacerlo dependerá del teléfono y de su sistema operativo. Además pueden acceder a teléfonos bloqueados explotando vulnerabilidades de seguridad en el teléfono. Por ello, el uso de estas herramientas puede constituir una forma de «hacking».

¿Qué hacen las herramientas de extracción de teléfonos móviles?

Las herramientas de MPE son dispositivos que permiten a la Policía a extraer datos de los teléfonos móviles, incluyendo:

- contactos;
- datos de llamadas (es decir, a quién se llama, 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 metadatos en estas aplicaciones);
- historial de geolocalización;
- conexiones a redes wifi (que pueden revelar las ubicaciones de cualquier lugar donde te hayas conectado a una red wifi, como tu lugar de trabajo o una cafetería).

4 Movile Phone Extraction (siglas en Inglés).

Algunas herramientas MPE también pueden acceder a datos almacenados en la nube (por lo que, aunque tengas mucho cuidado de minimizar los datos almacenados en tu dispositivo, se puede acceder a ellos si están almacenados en línea), o a datos que ni siquiera sabes que existen, e incluso a datos borrados. Por ejemplo, desde TEDIC hemos confirmado la adquisición de un software MPE por parte del Ministerio Público, que utiliza el equipamiento UFED[5] para análisis forense de dispositivos desde el año 2014[6].

Por otro lado, el Ministerio del Interior se negó[7] a responder la consulta pública por criterios de seguridad nacional. La Policía Nacional[8] y el Ministerio de Defensa han alegado que no cuentan con tales dispositivos.

¿Cómo puede la Policía utilizar las herramientas de extracción de teléfonos móviles en una manifestación?

- Para extraer los datos almacenados en él, la policía tendría que acceder físicamente a tu teléfono móvil.
- 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 (incluyendo el teléfono celular).
- En algunos casos, la policía también podría llevarse tu teléfono, si fuiste testigo o incluso víctima de un delito.
- En Paraguay, las instituciones de persecución penal (Ministerio del Interior, Agencia de Inteligencia, Fiscalía) cuentan con estas herramientas de extracción y análisis de dispositivos móviles. Sin embargo, para poder utilizarlas necesitan de una autorización judicial previa.

Lo que hay que tener en cuenta al acudir a una manifestación

- Mantener el sistema operativo de tu teléfono (Android o iOS) actualizado, lo que significa que tendrá las últimas funciones de seguridad. Esta es probablemente la mejor manera de prevenir el MPE.
- Aunque la forma más eficaz de protegerse contra el MPE es no llevar el teléfono a una manifestación, es poco probable que esta sea una solución realista. De hecho, no tener tu teléfono puede dejarte vulnerable de otras maneras.

---

5 *Cellebrite*, compañía de Israel se dedica a fabricar y vender estos dispositivos capaces (según afirman oficialmente https://cellebrite.com/en/cellebrite-introduces-ufed-touch2-platform/) de «extraer» datos de los dispositivos móviles que se conecten a ellos con una «solidez forense». Más información: https://cellebrite.com/en/about/ En el 2020, la empresa de mensajería *Signal* publicó algunas de las vulnerabilidades del software *Cellebrite* y ha puesto en duda la veracidad de las extracciones de datos. https://signal.org/blog/cellebrite-vulnerabilities/

6 Respuesta del Ministerio Público sobre consulta pública de análisis de los dispositivos (2021): https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/48148

7 Respuesta del Ministerio del Interior sobre consulta pública de análisis de los dispositivos (2021): https://informacionpublica.paraguay.gov.py/public/1719973-resolucin615pdf-resolucin615.pdf

8 Respuesta de la Policía Nacional sobre consulta pública de análisis de los dispositivos (2021): https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/48142

- Si bien deberías mantener tu teléfono bloqueado, algunas herramientas de MPE están diseñadas para acceder incluso a teléfonos bloqueados. Sin embargo, su capacidad para evitar esta medida seguridad depende del teléfono y de su sistema operativo.
- Antes de ir a una manifestación, 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. Pero debes tener en cuenta que cuando la Policía tome tu dispositivo, los mismos pueden haber sometidos a algunas herramientas de MPE, que son capaces de recuperar los datos borrados. Si guardaste los datos en un servicio en la nube, algunas herramientas MPE pueden seguir accediendo a esos datos.
- En caso que la policía haya tomado tus dispositivos. Y sospechas que hayan utilizados algunas de estas herramientas. Se sugiere adquirir otro dispositivo. Luego del *hacking* el dispositivo queda vulnerable o inseguro y se puede convertir en un objetivo de ataques por parte de otras personas. Entonces, si te devuelven el teléfono, puede ser inseguro que lo sigas utilizando.

¿Cómo se pueden utilizar los receptores IMSI en una manifestación?

¿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. Estos son 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).
- 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.
- IMSI es el acrónimo de International Mobile Subscriber Identity: es la clave de servicio del suscriptor y consiste en un número único para tu tarjeta SIM. Los receptores IMSI también se conocen como «Stingrays».
- Otros identificadores: hay algunos otros componentes en tu teléfono con identificadores únicos, como la dirección MAC de tu antena wifi, el Bluetooth Device Address (BD_ADDR) o el identificador de publicidad.
- En Paraguay, 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.

¿Qué es un receptor IMSI?

- IMSI es el acrónimo de International Mobile Subscriber Identity: es la clave de servicio del suscriptor y consiste en un número único para tu tarjeta SIM.
- Un receptor IMSI es un dispositivo que localiza y rastrea todos los teléfonos móviles que están conectados a una red telefónica en su proximidad, «capturando» el número IMSI único de cada dispositivo.
- Lo hace simulando ser una torre de telefonía móvil, «engañando» a los teléfonos móviles cercanos para que se conecten a él, 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 más accesible es tu ubicación. A través de las torres de telefonía se pueden conocer la distancia de un dispositivo por fuerza de la señal del mismo y las antenas, y así conocer tu ubicación aproximada a través de la triangulación de las mismas; de hecho, así es como te proporcionan su servicio en primer lugar. Al interponerse entre vos y la torre de telefonía, un receptor IMSI puede averiguar tu ubicación aproximada.
- Los receptores IMSI no leen los datos almacenados en el teléfono. Sin embargo, estos dispositivos pueden utilizarse para intentar interceptar mensajes de texto plano (SMS) y llamadas telefónicas.
- 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 intercambias a través de plataformas que utilizan cifrado (por ejemplo, Signal, WhatsApp, Telegram[9], Element, Wire).

¿Cómo podrían utilizarse los receptores IMSI en una manifestación?

- La policía puede utilizar los receptores IMSI[10] para identificar quién estuvo en una manifestación, capturando los números IMSI de todos los teléfonos que estuvieron en proximidad a esa manifestación. 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 llamadas y mensajes.

---

9 Telegram no tiene E2E en las comunicaciones por defecto. Sin embargo, el transporte sí está cifrado, esto implica que entre el teléfono y los servidores de Telegram están cifrado y no permite la interceptación de terceros.

10 En la actualidad no sabemos con certeza si la policía y los sistemas de seguridad paraguayos están usando receptores IMSI con este tipo de capacidades. Como la policía afirma «no poder confirmar ni desmentir» el uso de receptores IMSI, es difícil determinar qué tipo de receptores están usando.

¿Qué debes tener en cuenta al ir a una manifestación?

- Si querés evitar que el contenido de tus mensajes de texto sea rastreado por un receptor IMSI, puedes utilizar servicios de mensajería con cifrado, como Element, Signal y WhatsApp. La única información que un receptor IMSI podría recoger es el hecho de que estás utilizando estas aplicaciones de mensajería, no el contenido en sí.
- Aunque los receptores IMSI no leen los datos almacenados en el teléfono, tené en cuenta que la policía dispone de otras tecnologías que le podrían permitir acceder a los datos de tu teléfono, como la «extracción de teléfonos móviles» y otras herramientas de hackeo.
- También una opción es que no necesites comunicarte durante la manifestación. Poné tu teléfono en modo avión o apagalo por completo hará que un receptor IMSI no pueda rastrearte ni a vos ni a tus comunicaciones.

¿Por qué te debe importar?

Los receptores IMSI suponen una enorme invasión del derecho a la intimidad: engañan a todos los teléfonos móviles de una zona determinada para que den información sobre su propietario, incluso durante lo que la policía podría describir como operaciones «selectivas». Estos dispositivos recopilan los datos personales, pero la policía se niega a revelar qué hacen con ellos, cuánto tiempo los conservan o con quién los comparten.

Cuando un receptor IMSI intercepta las llamadas, los mensajes de texto o el tráfico de Internet de tu teléfono, esto representa una invasión aún más extraordinaria de tu privacidad. Al combinar los datos de tu teléfono con otra información, el gobierno no sólo puede identificarte, sino también empezar a rastrearte y construir un perfil sobre vos.

No es sólo tu derecho a la intimidad el que está amenazado, sino tu derecho a la libertad de expresión y libertad de manifestación pacífica en espacios públicos.

¿Cómo la policía puede determinar tu ubicación y cómo podés controlar el acceso a tus datos de localización?

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

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

Ubicación por GPS

- El GPS (Sistema de Posicionamiento Global) utiliza la navegación por satélite para localizar tu teléfono con bastante precisión (en un rango de pocos metros), y se basa en un chip GPS dentro de tu teléfono.
- Dependiendo del teléfono que utilices, tus 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.

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 tan pronto estés conectado a la red. Es decir, cuando tu teléfono está encendido y no en modo avión. Esta técnica 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 internet.

También se pueden utilizar otros métodos para determinar tu ubicación de forma indirecta, como los puntos de acceso wifi abiertos y las balizas bluetooth[11] a las que se conecta tu teléfono o los metadatos de ubicación incrustados en tus fotos.

¿Cómo se puede acceder a mis datos de localización?

Hay una serie de métodos que la policía puede utilizar para acceder al historial de ubicación (del teléfono):

Datos de GPS

- El acceso a los datos de localización del GPS puede hacerse mediante un dispositivo de «extracción de teléfonos móviles», que se conecta a tu teléfono movil y descarga todos los datos almacenados en él, incluidos los detalles de los lugares que has visitado.
- Este acceso a datos, también puede lograrse hackeando tu dispositivo: técnicas avanzadas que podrían no requerir el acceso físico a tu teléfono y podrían aplicarse de forma remota.
- Si tus datos GPS también están almacenados en una cuenta online (por ejemplo, iCloud o Google Maps), se podría acceder a ellos a través de tecnologías de extracción en la nube o de solicitudes legales a las empresas que almacenan esos datos.

Datos de localización de la red móvil

- La policía puede acceder a tus datos de localización aproximados a través de un pedido de orden judicial previa a tu proveedor de servicios.
- Esto significa que la policía no necesita acceder a tu dispositivo móvil para determinar que estuviste a cierta distancia de una manifestación.
- 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 móviles encendidos y conectados a una red móvil en una zona específica. Simulando ser una torre de celular, permite extraer información de ciudadanos en manifestaciones, reuniones o eventos públicos, con el fin de obtener información acerca de las personas que asisten.

---

11 Dispositivo transmisor que se utiliza para radiar una señal bluetooth de baja energía (LE) a dispositivos móviles que se encuentren cerca de él sin necesidad de sincronización previa. Esta tecnología permite a teléfonos inteligentes, ordenadores o tabletas ejecutar determinadas acciones cuando entran en el radio de una de ellas.

Cómo controlar mejor tus datos de localización

Controlar datos de GPS

- La mejor manera de evitar que se acceda a tu ubicación es limitar la generación de los datos de localización.
- En el caso del GPS, puede ser tan sencillo como apagar tu GPS (a menudo denominado «servicios de localización»). Pero ten en cuenta que los datos de localización de cualquier ocasión anterior en la que estuviera activado podrían seguir siendo accesibles.
- Si todavía necesitas usar el GPS en tu teléfono, comprueba los permisos de las aplicaciones individuales para acceder a tu ubicación y así minimizar el almacenamiento de estos datos.
- Además, eliminar los permisos de acceso a tu ubicación puede evitar que estos datos se almacenen en una cuenta online.
- Si es absolutamente necesario que una aplicación tenga acceso a tus datos GPS, inspecciona la configuración de esa aplicación para asegurarte de que entiendes 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 has tomado 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.

Controlar datos de localización de la 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.
- Tener el teléfono apagado, en modo avión o en una jaula de Faraday[12] impedirá 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.

12 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.

¿Cómo se puede utilizar el monitoreo de las redes sociales en una manifestación?

¿Qué es el monitoreo de las redes sociales?

- El monitoreo de las redes sociales se refiere al seguimiento, la recopilación y el análisis de la información compartida en las plataformas de las redes sociales, como Facebook, TikTok, Twitter, Instagram y Reddit.
- 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 compartes).
- Mediante el scraping y otras herramientas, 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 Paraguay existen prácticas de monitoreo en redes sociales[13] por parte de las autoridades, sin una regulación específica, ni debido proceso. Estas técnicas pueden ser inconstitucionales.

¿Cómo se utiliza el monitoreo de las redes sociales en relación a las manifestaciones?

- Los organizadores de las manifestaciones suelen utilizar las redes sociales para organizarlas, comunicarse con los manifestantes y subir fotos y vídeos de las mismas.
- Esto significa que la policía puede 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, así como otra información relacionada.
- La policía puede rastrear publicaciones en redes sociales relacionadas con protestas pasadas o futuras para identificar a los manifestantes[14].
- También podrían aplicar tecnologías de reconocimiento facial o de reconocimiento de movimientos corporales (gait recognition) a las imágenes y vídeos de las manifestaciones subidos a las redes sociales para identificar a los manifestantes.

---

13 Mujer que amenazó contagiar COVID-19 utilizando redes sociales, fue imputada por el Ministerio Público. https://www.abc.com.py/nacionales/2020/03/31/mujer-que-amenazo-con-contagiar-covid-19-se-expone-a-pena-de-tres-anos/

14 La justicia paraguaya solicitó extradición a manifestantes que quemaron la bandera y pintaron el panteón de los héroes. Las mismas fueron identificadas a través de las redes sociales. https://www.abc.com.py/nacionales/2021/02/18/juez-solicito-extradicion-de-jovenes-que-quemaron-bandera-paraguaya-y-pintaron-panteon-de-los-heroes/
La estudiante y representante estudiantil Vivian Genes y otros fueron procesados judicialmente por participar en una protesta pacífica ante la ANR y supuesta quema de su sede. Ella fue identificada a través de las redes sociales http://ea.com.py/vivian-genes-injustamente-apresada-es-una-de-las-artifices-del-movimiento-arancel-0/

¿Qué debes tener en cuenta al ir a una manifestación?

- Si subes tus imágenes de la manifestación a tus cuentas de redes sociales, pueden ser utilizadas para identificar y ubicar a las personas en el lugar de la manifestación.
- Si la configuración de la ubicación está activada en tus plataformas de redes sociales o en tus aplicaciones de cámara y fotografía, y luego publicas en línea desde o cerca del lugar de una manifestación, la policía puede tener acceso a esos datos de ubicación.
- Si quieres utilizar las redes sociales mientras estás en una manifestación, deberías considerar la posibilidad de desactivar los ajustes de localización en las plataformas que vayas a utilizar. Si decides compartir imágenes de la manifestación, 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 manifestación.
- Si quieres subir tus imágenes de la manifestación a las cuentas de las redes sociales, considera 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.
- Las imágenes pueden seguir siendo geolocalizadas a partir de información de contexto (por ejemplo, un monumento o punto de referencia). Al hacer grabaciones ten en cuenta eso y evita la identificación contextual.

¿Cómo se puede utilizar el hackeo en las manifestaciones y cómo se puede minimizar su riesgo?

¿Qué es el hackeo?

- El hackeo se refiere a la búsqueda de vulnerabilidades en los sistemas electrónicos, ya sea para reportarlas y repararlas, o para utilizarlas en un ataque.
- El hackeo comprende una serie de técnicas en constante evolución. Pueden hacerse de forma remota, pero también pueden incluir la interferencia física con un dispositivo o sistema, por ejemplo, forzando el desbloqueo de tu teléfono móvil.
- También puede consistir en aprovecharse de las personas para acceder a sus dispositivos o cuentas. Un ejemplo de ello es el «phishing»[15], en el que un atacante se hace pasar por una persona u organización de confianza para enviar un enlace o archivo adjunto infectado con malware.

15 El *phishing* es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial a través de mensajes de SMS, chat de mensajerías, correos electrónicos, llamadas telefónicas, entre otros.

¿Cómo se puede utilizar el hackeo en las manifestaciones?

- La policía puede hackear las comunicaciones utilizando, por ejemplo, receptores IMSI. Pero los receptores IMSI sólo pueden interceptar la información que se transmite entre un dispositivo móvil y una torre de telefonía: no pueden acceder a la información que se almacena en el dispositivo.
- Por lo tanto, la policía puede utilizar técnicas sofisticadas de hackeo para obtener acceso remoto a la información almacenada en tu dispositivo[16]. Esto podría ocurrir incluso si están protegidos con contraseña, huella dactilar o desbloqueo facial.
- La policía también puede recoger y acceder a cualquier dispositivo que se les caiga, pierda o confisque a los manifestantes en una manifestación.

¿Qué debes tener en cuenta al ir a una manifestación?

- Mantené tu dispositivo actualizado. Es una buena forma de prevenir la piratería informática, ya que esta suele aprovechar las vulnerabilidades que se han revelado pero que aún no han sido corregidas.
- Asegúrate de que tu dispositivo ejecuta la última versión disponible de su sistema operativo (Android o iOS) y que todas tus aplicaciones están actualizadas para mejorar tu seguridad y minimizar el riesgo de hackeo.
- Aunque deberías mantener tu teléfono u otros dispositivos electrónicos bloqueados, algunas técnicas de hackeo pueden sobreponerse a este obstáculo. Su capacidad para saltarse esta seguridad, sin embargo, depende de la técnica de hackeo utilizada y del dispositivo al que se dirige.
- Antes de ir a una manifestación, puedes considerar hacer una copia de seguridad de los datos de tu teléfono en otro dispositivo, y luego eliminar esos datos de los dispositivos que lleves contigo. Pero debes tener en cuenta que algunas herramientas de hackeo son capaces de recuperar los datos borrados. Si has guardado los datos en un servicio en la nube, algunas herramientas de hackeo pueden seguir accediendo a esos datos.
- Siempre debes tener cuidado con los enlaces en los que haces clic, para evitar ataques de «phishing».

16 En la investigación sobre vigilancia de las comunicaciones en Paraguay se detallan las adquisiciones que ha hecho el Estado para acceder de forma remota a dispositivos: https://www.tedic.org/paraguay-debe-de-elevar-sus-estandares-de-proteccion-de-las-comunicaciones-privadas/


ACAB

VIGILANCIA DE TU ROSTRO Y TU CUERPO

¿Cómo puede utilizarse la tecnología de reconocimiento facial en una manifestación y cómo puedes intentar mantener tu anonimato?

¿Qué es la tecnología de reconocimiento facial?

- El reconocimiento facial funciona mediante un software alimentado por un algoritmo (una fórmula) que está entrenado para reconocer rostros e individualizar sus rasgos.
- La tecnología de reconocimiento facial (TRF) recopila y procesa datos sobre los rostros de las personas y puede utilizarse para identificarlas. Funciona comparando las imágenes capturadas con las almacenadas en las bases de datos existentes o en las «listas de vigilancia». 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.
- 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 Paraguay esta tecnología ya se encuentra en funcionamiento en varias ciudades del país. Por ejemplo se instalaron cámaras de reconocimiento facial en zonas fronterizas[17], Asunción[18], Encarnación[19], Pedro Juan Caballero[20], entre otras ciudades[21].
- TEDIC solicitó información pública sobre las instalaciones de TRF en Asunción y su tratamiento de datos. La solicitud fue denegada por el Ministerio del Interior y actualmente se encuentra en litigio[22] ante la Justicia.

---

17 Migraciones implementa nueva tecnología biométrica con reconocimiento facial para el control del tránsito vecinal fronterizo en el Puente de la Amistad (2020). http://www.migraciones.gov.py/index.php/noticias/migraciones-implementa-nueva-tecnologia-biometrica-con-reconocimiento-facial-para-el-control-del-transito-vecinal-fronterizo-en

18 Biometría y video-vigilancia en Asunción. https://www.tedic.org/biometria-y-video-vigilancia-parte1/ y https://www.tedic.org/biometria-y-video-vigilancia-la-enajenacion-continua-de-nuestros-derechos-parte-2/

19 Se instalan 80 cámaras en la ciudad de Encarnación: 10 de ellas son de reconocimiento facial y 10 de reconocimiento de placa de vehículos. https://www.lanacion.com.py/pais_edicion_impresa/2019/09/02/encarnacion-instalaron-80-camaras-de-vigilancia/

20 Se instalan en la capital de Amambay: 8 cámaras de reconocimiento facial y 12 de reconocimiento de placas de auto. https://www.lanacion.com.py/pais/2019/09/04/sistema-911-se-instala-por-primera-vez-en-pedro-juan-caballero/

21 Esta tendencia de adquisición de software de reconocimiento facial es regional. Ver informe de ALSUR 2021: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia

22 Quién vigila al vigilante: reconocimiento facial en Asunción (2019). https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/

¿Cómo podría utilizarse en relación con una manifestación?

- La TRF puede utilizarse para vigilar, rastrear e identificar los rostros de las personas en los espacios públicos, incluso en las manifestación. Esto puede hacerse abierta o furtivamente, sin que las personas lo sepan o lo consientan.
- Las cámaras con tecnología TRF pueden tomar fotos o vídeos e identificar a las personas en tiempo real o en un momento posterior. La TRF también puede utilizarse para analizar e identificar imágenes existentes, por ejemplo, fotos y vídeos de manifestaciones subidos a las redes sociales.
- A medida que se recogen los datos faciales de los manifestantes, pueden añadirse a una o más «listas de vigilancia» preexistentes, donde pueden compararse con los datos faciales de otras fuentes para encontrar una coincidencia.
- Estos datos también podrían utilizarse para crear una nueva base de datos de personas que asisten a las protestas, con el fin de realizar futuras comparaciones e identificaciones.

¿Qué debes tener en cuenta al ir a una manifestación?

- Si quieres intentar mantener tu anonimato, puedes considerar la posibilidad de llevar la cara cubierta, por ejemplo con un pañuelo, lo que puede dificultar que la TRF capte imágenes precisas de tus rasgos faciales.
- Otras opciones para interrumpir la TRF incluyen el uso de pintura facial y ropa con diseños destinados a interferir con el reconocimiento facial preciso. Sin embargo, la TRF se adapta y mejora constantemente, por lo que las pinturas faciales y estos otros métodos pueden resultar menos eficaces en el futuro.
- Las facultades de la policía para exigir el retiro de tales cubiertas y ropas varían según el contexto y la jurisdicción. En el momento de escribir este artículo, estamos en medio de la pandemia de la COVID-19, por lo que las normas actuales pueden estar sujetas a cambios.
- Dado que la policía puede utilizar la TRF para analizar imágenes o grabaciones de vídeo en las redes sociales, considera esto cuidadosamente antes de publicar cualquier imagen de una manifestación en la que aparezcan los rostros de otros manifestantes.
- Por lo tanto, es posible que quieras considerar el uso de herramientas de difuminación de rostros antes de publicar fotos o vídeos en línea.

Cámaras corporales en una manifestación

¿Qué hacen las cámaras corporales?

- Las cámaras corporales pueden fijarse a la ropa de un agente de policía —a menudo a la altura del pecho, los hombros o la cabeza— y grabar video, incluido el sonido, desde la perspectiva del agente.
- Las cámaras corporales probablemente serán visibles para vos, y cuando estén grabando, debería aparecer una luz intermitente en el dispositivo.

¿Cómo podrían utilizarse las cámaras corporales en una manifestaciones?

- Las cámaras corporales pueden utilizarse en las manifestaciones para controlar las acciones de los manifestantes.
- No suelen captar las propias acciones del agente de policía.
- Fuera del contexto de las protestas, las cámaras corporales normalmente se encienden sólo al comienzo de un incidente. Pero en una manifestación, pueden permanecer encendidas durante todo el tiempo.
- Algunas cámaras exigen que el video se cargue manualmente en un servidor, pero algunas de las cámaras corporales más recientes permiten que las imágenes se transmitan en directo a una comisaría.
- Aunque en Paraguay no cuenta con información de que se utilicen de esta forma, la grabación podría ser procesada posteriormente, por ejemplo, mediante un software de reconocimiento facial.[23]

¿Qué debes tener en cuenta al ir a una protesta?

- Aunque la Policía Nacional, por ejemplo, afirma que las cámaras de corporales actúan como «testigos independientes», los agentes de policía individuales 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.

¿Cómo se pueden utilizar drones policiales en una manifestación y cómo se puede intentar mantener el anonimato?

¿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 podrían estar habilitados con tecnología de reconocimiento facial.
- Los drones pueden estar equipados con altavoces, equipos de vigilancia, radares y herramientas de interceptación de comunicaciones, como los receptores IMSI.
- En Paraguay, el Ministerio del Interior ha adquirido drones para la vigilancia en tiempos de pandemia de la COVID19[24].

---

23 La Policía Nacional presentó la utilización de las *bodycam* (cámaras corporales), en el marco de lo establecido en la Ley 6.699, que determina el uso obligatorio de tapabocas para la prevención de la pandemia de COVID-19. Los agentes llevarán cámaras incorporadas al uniforme para dar registro a todos los procedimientos que se realicen en la ciudad, en especial para el cumplimiento de las medidas sanitarias (2021). https://www.lanacion.com.py/pais/2021/01/09/policia-nacional-presento-camaras-corporales-que-usaran-en-procedimientos/

24 Uso de drones: ¿combaten la pandemia o refuerzan el control a la ciudadanía (2020) https://www.tedic.org/uso-de-drones-covid19/

¿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 su consentimiento.
- Del mismo modo, cuando están equipados con tecnologías de interceptación de las 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.
- Los drones equipados con altavoces también pueden utilizarse para comunicarse con los manifestantes, por ejemplo, dándoles órdenes, instrucciones o advertencias[25].

¿Qué debes tener en cuenta al ir 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.

25 No sabemos con certeza qué tipos de capacidades tienen los drones usados por la Policía Nacional paraguaya.

TE
DIC·
TECNOLOGÍA &
COMUNIDAD