Guía

El smartphone y la militancia

Colectivo 406

Editado en mayo de 2024.

Texto original:
https://406.neocities.org/a/smartphone_y_militancia

ÍNDICE

El smartphone

El smartphone lleva poco entre nosotros y ya es un apéndice de nuestro cuerpo. Seguramente estemos ante la revolución antropológica más rápida de la historia, tan rápida que en el plazo de una década hemos normalizado llevar un ordenador en el bolsillo y casi sentirnos desnudos cuando no lo llevamos encima. Si hemos llegado a esta situación, es por las ventajas que nos ofrece este dispositivo, principalmente la de conectarnos al mundo, al instante y sin esfuerzo. El capitalismo inaugura una época en la que todas las partes del globo entran en interdependencia mutua y, pese a las diferencias culturales e idiosincráticas de cada lugar, se igualan las relaciones económicas y políticas. En vista de lo anterior, creemos que no es exagerado afirmar que si el smartphone se transforma en parte indispensable de nuestras vidas es precisamente por ser la herramienta que nos concede pleno acceso a este contexto cosmopolita.

Sin embargo, con la fusión antropológica entre esta máquina y nuestro cuerpo, nos hemos convertido en nodos del llamado Internet de las Cosas (IoT). Ahora, nuestro cuerpo emite, recibe, tiene sensores, micrófono, cámara y, en general, genera datos e información. Tantos datos y tanta información que las empresas que actualmente lideran el mercado capitalista son las Big Tech, cuyo negocio está en los datos, que tan abundantemente ofrecemos, gratis y sin hacer nada más que navegar la red y usar aplicaciones. El negocio quedó servido y ahora nuestros datos valen oro.

Con esta fusión, también **hemos heredado las vulnerabilidades de la máquina**, relacionadas principalmente con el control social. Las novelas distópicas del siglo XX, escritas cuando no solo no existía el smartphone, sino que ni siquiera existía el ordenador, relatan historias en sociedades donde los mandatarios todo lo ven y todo lo oyen, mediante medios que hoy nos parecen arcaícos, donde el gobierno es más semejante a un panóptico que a un ágora. Con el smartphone, se hace realidad este sueño húmedo de cualquier institución que ejerce o aspira a ejercer un ferreo control social sobre la población. Pero la población es un concepto abstracto y el dominio no puede comprenderse si se achaca a la maldad de unos pocos. Por eso, decimos que **el smartphone es una herramienta de control social masivo al servicio del capital**, que sirve a los Estados capitalistas para vigilar y castigar y, en definitiva, para preservar una sociedad donde el dominio del capital sobre el trabajo es la regla esencial. No es que haya sido concebido específicamente para ejercer esta función. El smartphone es un producto de mercado, destinado como tal a generar beneficio y, por tanto, tiene que ser un valor de uso para el consumidor y casar con sus necesidades, tales como hablar con la familia, amigos o pareja, comunicarse en el trabajo, crear contenido, consumir entretenimiento, facilitar trámites, etc. Es un dispositivo muy útil, por eso lo utiliza todo el mundo. Pero esto no quita que tenga lados negativos, muchos de ellos relacionados con adicciones y trastornos psicológicos (ansiedad, depresión...), otros relacionados con estafas y, lo que aquí nos interesa, el control social, específicamente aquel que se ejerce sobre la militancia revolucionaria.

El smartphone es un pequeño ordenador portátil, con una arquitectura un poco diferente y una pantalla táctil en vez del

clásico teclado y ratón. Como tal, está compuesto de hardware y de software. Dos son los principales sistemas operativos para móviles: Android e iOS. El primero está basado en Linux y es de código abierto, aunque es propiedad de una empresa privada (Google). El segundo, de código totalmente cerrado y privativo, propiedad de Apple. Pese a que Android sea de código abierto, la absoluta mayoría de los dispositivos Android del mercado traen instalada la versión privativa de Android de Google. Es decir, aquella versión que trae programas y binarios de Google, haciendo dependiente el dispositivo de una cuenta de Google, de la Google Play Store, etc. Algunos incluso traen consigo programas preconfigurados o drivers del fabricante, como Samsung, Huawei, Xiaomi, etc. Todo específicamente diseñado para recoger la mayor cantidad de datos posible del uso y preferencias del usuario. Con Apple ocurre directamente la peor situación, que es la de no saber bien qué funciones desempeña el sistema operativo, cómo funcionan los programas y, en general, todos los problemas que siempre se derivan del software y hardware privativo. Con el hardware la situación es incluso peor en ambos tipos de dispositivos, ya que leyendo la ficha técnica de las placas no se puede saber con exactitud la funcion de cada componente, dificultando tambien la reparación y reciclaje de estos.

Luego tenemos la red móvil que, al igual que Internet, está compuesta por routers, switches, cables e infraestructuras de empresas privadas, que no escatiman en recursos para ejercer una hipervigilancia promovida por los Estados. El smartphone, si quiere conectarse a la red móvil, es dependiente de una tarjeta SIM (ligada al número de identificación fiscal de la persona física en cada país), por lo que es muy fácil saber dónde está

o ha estado una persona. Las llamadas y los SMS no son nada privados y no es necesario pinchar el dispositivo para escuchar las conversaciones, el historial de llamadas queda guardado y es fácil registrar el historial de la navegación por Internet. Es más, todos estos datos se utilizan frecuentemente en juicios, como pruebas que no suelen arrojar duda alguna.

Las alternativas de código abierto y de vocación respetuosa con la privacidad, como LineageOS, PinePhone o Librem, presentan diferentes problemas como precios elevados, poca fiabilidad, problemas de seguridad, mal funcionamiento o la obligacion de utilizar drivers privativos que al usuario final no le causan más que problemas. Una mejor alternativa de software libre y enfocado a la seguridad es GrapheneOS. Afirmamos incluso que actualmente GrapheneOS es la única solución al problema de la seguridad en los smartphones, siendo incluso más seguro que cualquier sistema operativo de ordenador y 100% software libre. El principal y casi único inconveniente es que solo se desarrolla en una única gama de smartphones, que son los Pixel de Google, ya que es el único hardware que ofrece *verified boot* y otros requisitos de seguridad. El "problema" como tal no está en que el dispositivo sea de Google, ya que al instalar GrapheneOS se borra todo software de Google (quedando algo de firmware, que en principio no supone un problema). Además, hay que recordar que no es lo mismo la privacidad que la seguridad: los Pixel son a nivel de hardware los dispositivos más seguros del mercado, aunque de fábrica vengan con software de Google instalado, que es poco respetuoso con la privacidad. Al instalar GrapheneOS, eliminamos este software de Google. El problema, por tanto, es la obligatoriedad de disponer de un Pixel para poder instalar GrapheneOS, lo que limita la

gama de dispositivos en los que se puede instalar y, además, la platafoma hardware no es de código abierto. Aunque, es justo mencionar, los desarrolladores de GrapheneOS no están cerrados a desarrollar en otras plataformas, incluso de código abierto, pero siempre bajo la condición de que el hardware cumpla con unos mínimos de seguridad.

El smartphone en la militancia

Este tema es muy amplio y daría para largo. Ahora, siguiendo nuestros principios, nos queremos centrar en las repercusiones que el smartphone tiene en la militancia. Sobre todo, nos centramos en la repercusiones negativas relativas a la seguridad, ya que las facilidades y los aspectos positivos son evidentes, hasta el punto de que en diversos espacios militantes a menudo se tienen que poner límites en el uso del smartphone, porque facilita tanto la labor militante que muchas veces nos olvidamos de reflexionar sobre los problemas que nos puede suponer su uso.

Explicaremos los principales problemas y vectores de ataque a los que nos vemos expuestos con el uso de los smartphone y propondremos soluciones para mitigar estos riesgos, aunque, como siempre, no sean 100% infalibles.

Geolocalización

Nada hay más sencillo para la policía y los proveedores de telefonía que saber dónde se encuentra un smartphone. Saber dónde ha estado una persona da mucha información y a nivel jurídico suelen pasar fácilmente de indicios a pruebas. Si hemos estado en un evento, si hemos asistido a una reunión, dónde nos reunimos habitualmente, si hemos estado pegando carteles, nuestra asistencia a una manifestación, la frecuencia con la que nos reunimos con determinadas personas, etc. Todo eso es fácil de averiguar si hemos llevado el smartphone encima. Los métodos son varios:

- **GPS:** es evidente que un servicio de geoposicionamiento puede revelar dónde estamos o hemos estado. El sensor GPS es pasivo, es decir, solo recibe datos, por lo que no es el problema en sí. Lo que pasa es que las aplicaciones que lo usan suelen enviar estos datos a sus servidores y una petición judicial a las empresas que los gestionan puede servir para extraer esos datos.
- **Antenas de telefonía:** curiosamente, sirven más para geolocalizar un dispositivo móvil que el GPS. Esto sucede porque el dispositivo móvil, si no está en modo avión o apagado, se comunica continuamente con las antenas de telefonía, para dar acceso a la red móvil y de datos (Internet móvil). Con técnicas de triangulación se puede saber de forma modestamente exacta la localización de un móvil, en el presente o en el pasado.
- **WiFi y Bluetooth:** los módulos de WiFi y Bluetooth de los smartphone envían y reciben datos continuamente cuando están activados, con el objetivo de descubrir puntos de acceso o dispositivos cercanos. Teniendo en cuenta que ambos disponen de un identificador único llamado MAC, pueden usarse para rastrear donde ha estado un dispositivo (GrapheneOS tiene una funcionalidad que randomiza la MAC por cada conexión, para evitar eso). Por ejemplo, desplegando sensores por toda la ciudad (cosa que se está haciendo en algunos sitios) o en manifestaciones (algo que se ha llegado a hacer desde helicópteros).
- **Conexión a Internet:** cuando el smartphone se conecta a Internet, ya sea vía datos móviles o ya sea por WiFi, revela

a través de su IP de salida la localización del smartphone. Esto mismo ocurre con cualquier ordenador. En el caso de hacerlo vía datos móviles, no nos sirven ni las VPN ni la red Tor, ya que la empresa de telefonía va a saber que nos hemos conectado a una torre en específico, aunque luego no sepa exactamente qué estamos haciendo en Internet.

Visto lo visto, **la única solución realista contra la geolocalización es no llevar el smartphone encima**. Ahora bien, no hay que caer en paranoia. Lo que decimos es que no hay que llevar el dispositivo móvil encima cuando no se quiere que se sepa que hemos estado en un sitio. En general, no llevarlo a reuniones, a eventos políticos, a manifestaciones, a acciones, etc. Y si no llevarlo no es una opción, cosa que pasa a menudo, lo mejor es llevarlo apagado desde casa y encenderlo una vez nos hemos alejado del lugar problemático (esto solo nos protege si nuestro dispositivo no está infectado con spyware, como veremos más abajo). El modo avión es la siguiente opción, aunque no es fiable al 100% en dispositivos Android, porque, aunque la versión pura de Android funciona bien en este sentido, la correcta implementación del modo avión varía según el fabricante, debido a que introducen modificaciones a la versión base de Android, pudiendo producir fallos en partes del sistema, entre ellos el modo avión.

Sensores

Al smartphone solo le faltan brazos y piernas para ser un robot humanoide. Tiene ojos (cámara), oídos (micrófonos), voz (altavoces), sentido espacial (giroscopio, acelerómetro, sensor de luz), etc. Es más que evidente qué problemas puede acarrearnos tener un dispositivo con la capacidad de registrar diversos tipos

de datos a través de estos sensores, por lo que no nos extenderemos en explicarlos. Lo que sí merece la pena explicar es bajo qué condiciones pasan de ser meros sensores a sensores espías. Estos casos son dos.

El primer caso es el de las aplicaciones que, debido a su interés de negocio con los datos o a objetivos más "benévolos" como ayudar a mejorar la experiencia del usuario, recogen continuamente datos y métricas que se almacenan en servidores, se procesan y se usan para fines de lucro o simplemente técnicos, pero que, en todo caso, quedan almacenados y pueden ser objeto de petición judicial o cesión a agencias de inteligencia. Esto se hace y no es ningún misterio para nadie. El ejemplo más claro y conocido es el de Instagram, que tras tener una conversación sobre el embarazo comienza a mostrar anuncios sobre métodos anticonceptivos o ropa de bebé. La conversación puede ser tan inocente como esa o, en cambio, puede ser una conversación sobre cuándo y dónde es una reunión, qué se ha dicho en una reunión, cómo se llaman los integrantes de un colectivo, etc.

El segundo caso es el del spyware, tema que trataremos en un apartado específico, por ahora quedándonos con la idea de que si hay un programa espía en nuestro smartphone, los sensores se convierten en ojos y oídos al servicio de la policía o de la agencia de inteligencia.

Lo único que se puede hacer en este caso, como en casi todos, es **no llevar el smartphone a ningún espacio militante, ni manifestaciones, ni acciones y, sobre todo, no tener conversaciones comprometidas en presencia de un dispositivo móvil.**

Escuchas telefónicas

Es público y notorio que el Estado *pincha* las llamadas telefónicas en investigaciones donde hay una orden judicial que lo autoriza, lo cual es totalmente legal. Muchas veces no somos conscientes de que estamos siendo víctimas de una investigacion de este calibre. Existe también la posibilidad de pinchazos extra-judiciales y, lo peor de todo, es que son una práctica habitual y legal (dependiendo del país).

Luego está el factor del registro de llamadas, que es casi un estándar de los proveedores de telefonía: registros de quién llama a quién, cuándo y desde dónde. Estos datos se almacenan durante años. Aunque no lo sabemos a ciencia cierta, no nos debería extrañar que cualquier conversacion esté siendo preventivamente grabada, aunque seamos ciudadanos ejemplares, ya que técnicamente no supone una gran complicacion para las compañias telefónicas grabar absolutamente todas las llamadas existentes y acceder a ellas cuando haga falta.

Suponiendo que en nuestro smartphone no esté instalado un spyware, **siempre es mejor hacer llamadas por Signal u otra aplicación que provea llamadas cifradas por Internet**. **Las llamadas telefónicas de toda la vida no son seguras**. Hay que dejar de utilizarlas y no puede haber más discusión en este punto. El Nokia viejo que nos da aires de traficante no es más seguro que un smartphone de última generación.

Ahora bien, hemos dicho que esa solución solo aplica bajo el supuesto de que no estemos infectados por algún tipo de spyware policial. Por ello, **la información comprometida nunca se debe dar por llamadas**, por mucho que estén cifradas. Aunque, como sabemos que muchas veces es necesario llamar, si se hace,

siempre hay que hacerlo por Signal o por alguna aplicación segura de mensajería. Llamar por vía telefónica tradicional es, sin duda, una de las peores costumbres del uso militante del smartphone.

Mensajería

Seremos breves. Al igual que las llamadas, los SMS no son seguros. El contenido no está cifrado y en los servidores de la empresa de telefonía queda registrado el emisor, el receptor, el lugar, la fecha y el contenido.

La solución, de nuevo bajo el supuesto de que no estemos infectados por spyware, es utilizar aplicaciones seguras de mensajería intantánea, de las cuales la mejor es Signal. Una vez más, insistimos en la idea de que **no debemos comunicar información comprometida ni siquiera por Signal**, ya que existe la posibilidad de que tengamos spyware policial instalado en el smartphone.

Datos almacenados

Los datos que almacenamos en el dispositivo móvil son susceptibles de ser extraídos en caso de que caiga en las manos equivocadas.

Este caso suele darse en una situacion de detención policial, es decir, una vez que te han detenido o se te ha hecho una redada. También se puede dar cuando dejas el smartphone en algún lugar y un agente que te está haciendo un segimiento coge tu móvil, lo infecta y lo deja en el mismo sitio, aunque este tipo de ataque es mucho más específico y difícil.

Cuando requisan un dispositivo móvil, hay dos tipos de acciones que se pueden llegar a hacer. La primera sería intentar hacer un volcado de datos para ver todo el contenido del dispositivo. Para esto la policía dispone de maquinaria específica que incluso puede desbloquear el acceso al smartphone. No sabemos con exactitud la tecnología que posee la policía, pero la recomendacion principal es la de cifrar el dispositivo, función que los iPhone traen por defecto y que Android trae por defecto desde la versión 10. En caso de que tu dispositivo sea más antiguo, una simple búsqueda en Internet arroja muchas guías sobre cómo cifrar un smartphone, procedimiento que es muy sencillo. Aunque varía según el tipo de smartphone, la única situación en la que es 100% fiable que el dispositivo esté cifrado es cuando está apagado, ya que sitúa todos los datos cifrados at-rest. Si el dispositivo está encendido, puede tener los datos sin cifrar en la memoria volátil (RAM) e incluso el almacenamiento puede estar totalmente descifrado, bastando adivinar el desbloqueo de pantalla para poder acceder a ellos. Por tanto, siempre que creamos estar bajo peligro de detención o nos encontremos en alguna situación proclive a que nos detengan, es mejor llevar el smartphone apagado.

En cualquier caso, **siempre debemos buscar reducir el número de datos comprometidos que almacenamos en nuestro dispositivo.** Documentos secretos de nuestra organización, imágenes de militantes, conversaciones comprometidas, agitprop, contactos de nuestros camaradas, etc. Todo eso debe eliminarse tan pronto como no nos haga falta tenerlo almacenado. En cuanto a los contactos, siempre es mejor utilizar servicios de comunicación que utilicen nombres de usuario y no números de teléfono, ya que, como hemos dicho infinidad de

veces, estos sirven para identificar y relacionar a militantes. Se pueden usar servicios de mensajería como XMPP, Briar o Signal con los nombres de usuario. Sobre esto último, es mejor utilizar Molly, una modificación de la aplicación de Signal que implementa varias mejoras de seguridad, entre ellas el cifrado de la base de datos de los mensajes.

En resumen, las soluciones en este apartado son las de **reducir la cantidad de datos comprometidos que almacenamos, utilizar métodos de cifrado de los datos, apagar el dispositivo si estamos ante peligro y no llevar el dispositivo a eventos donde pueda sernos sustraído**. Si nos detienen y nos piden el pin o la contraseña de desbloqueo o descifrado del dispositivo, siempre alegaremos no recordarla o que la tenemos apuntada en algún papel (que habría que buscar, siempre existe la posibilidad de "haberlo perdido", etc.). También es recomendable no usar la huella dactilar como método de desbloqueo, porque, aunque en muchos países no te pueden obligar a ponerla en el sensor y desbloquear el dispositivo (tampoco a dar la contraseña), de sobra es conocido que la policía, cuando quiere, está por encima de la ley y bajo amenazas, tortura física y psicológica, puede conseguir lo que se propone.

También es importante mencionar que siempre existirá la posibilidad de que el cifrado pueda romperse (por mal diseño o algoritmo obsoleto) o de que el dispositivo tenga instalada una puerta trasera (backdoor) que permita descifrar los datos. Pero, como siempre decimos, es mejor aplicar todas las defensas a nuestro alcance y ponérselo difícil a la policía.

Spyware

Llegamos a la piedra angular de todo el edificio de defensas que podemos adoptar en este ámbito y del que ya hemos ido hablando en los anteriores apartados: el **spyware**. Este designa un **tipo de software diseñado para espiar al usuario del dispositivo donde está instalado.** Aunque muchas veces se confunden los términos, es una forma de decir que nos han pinchado el dispositivo móvil, es decir, que nos han instalado un software espía.

Si esto ocurriera, es bastante fácil deducir que todas las defensas que hemos ido proponiendo hasta ahora serían en vano, ya que todo lo que hiciéramos en el smartphone sería enviado a los servidores de la policía. El cifrado del dispositivo no nos salvaría de que pudieran ver nuestros datos descifrados. El uso de mensajería instantánea cifrada no serviría de nada, ya que leerían nuestros mensajes antes de cifrarse, ocurriendo lo mismo con las llamadas cifradas. Los sensores pasarían a enviar toda clase de telemetría para uso y disfrute de la policía. El spyware enviaría todos los datos que permitieran nuestra geolocalización y nos engañaría haciéndonos creer que hemos desactivado el GPS. Podría hacernos pensar que el dispositivo está apagado cuando en realidad está encendido. Lo mismo con el modo avión, el Internet, etc. Y ya, la guinda del pastel, directamente transmitir todo lo que muestra la pantalla. En un caso como este, en el que estuviéramos infectados o tuviéramos firmes sospechas de ello, **la única solución sería deshacerse del dispositivo.**

Los spyware son productos caros y en muchos casos se mide muy bien cuándo se usan y en qué sectores se priorizan, aunque

todo depende de los recursos que un Estado quiera dedicar al espionaje. También existe un *handicap* en este tema que consiste en la instalación del spyware, ya que no siempre es tan fácil como parece. Existen dos tipologías en cuanto a esto, que son la intervención física o la remota.

La intervención física es aquella mediante la que se instala el spyware a través del acceso físico directo al dispositivo. Ejemplos hay muchos. Cuando nos detienen, tienen nuestro dispositivo a mano para hacer lo que quieran. Un agente infiltrado en una organización puede instalarlo en un descuido de un militante, que se olvida el smartphone en alguna mesa. Pueden entrarnos en casa cuando no estamos en ella e implantarnos un sistema en el cargador del móvil para infectarlo cuando lo pongamos a cargar o lo mismo en el ordenador. Echarle imaginación basta para hacerse a la idea de las posibilidades que existen para infectar físicamente un dispositivo.

La intervención remota no requiere que la policía tenga acceso físico al dispositivo. La infección se suele hacer mediante la explotación de alguna vulnerabilidad remota del sistema operativo, de alguna aplicación que use el militante o mediante phishing, enviando un correo o un mensaje con un archivo convenciéndonos de abrilo que, al hacerlo, nos instala el spyware. La explotación de una vulnerabilidad remota no suele requerir de la interacción del usuario (*0-click*) o, a veces, se necesita poca. Ejemplos de este tipo pueden ser una simple llamada que, al cogerla, nos infecta o incluso puede que ni siquiera haya que cogerla. Lo mismo con un SMS o un mensaje de Whatsapp, etc. Las vulnerabilidades de este tipo son difíciles de encontrar y son muy cotizadas en el mercado negro. El caso del software espía Pegasus ha sido muy conocido en los últimos años y no es para menos. Este se instalaba remota-

mente, a través de un *exploit 0-click* (sin interacción del usuario) mediante Gifs de Whatsapp.

Como hemos dicho, son herramientas muy poderosas pero igual de caras y muchas veces difíciles de implantar, ya que en algunos casos con un simple reinicio se eliminan del dispositivo. Sin embargo, suele ser frecuente la inquietud en gran parte de la militancia, ante la idea de que puedan tener algún tipo de software espía instalado en su dispositivo móvil (o en el ordenador, el portátil, la tablet...) y al igual que decimos que todas las llamadas son muy fáciles de interceptar por parte de la policía, también tenemos que decir que estos casos son muy aislados. Hay que tener en cuenta que un software espía como Pegasus ya está anticuado y la implantación en un solo dispositivo, según los medios de comunicacion, puede costar entre 200.000 y 500.000 euros. La probabilidad de que tu información cueste estas cantidades de dinero son bastantes bajas. Aún así, **siempre es mejor prevenir que curar.**

Existen herramientas que pueden servirnos para despejar dudas y analizar smartphones en busca de spyware. PiRogue Tool Suite, es una distribución de Linux basada en Raspbian para Raspberry Pi (un mini-ordenador, para los no entendidos), con una configuración y herramientas preinstaladas que permiten analizar el tráfico de red de un smartphone con filtros específicos y analizar el contenido del mismo. Se crea una red WiFi desde la Raspberry Pi y conectando el smartphone a esta red durante un tiempo, PiRogue analiza el tráfico con reglas de Suricata, pudiéndo visualizar en varios gráficos de Grafana adónde va el tráfico del dispositivo móvil, qué peticiones hace, alertas de seguridad preconfiguradas, interceptar tráfico y un largo etcétera de funcionalidades que ayudan a determinar si el dispositivo está infectado o no.

Otra opción muy útil que ofrece PiRogue es Mobile Verifictaion Toolsuite (MVT). Es una base de datos creada por Anmistía Internacional en la que se almacenan rastros de software espía conocidos. Así, conectando el smartphone a la Raspberry Pi, podemos hacer una copia de seguridad de este y analizarla comparándola con esta base de datos y con diferentes patrones de configuración y alertas que tiene preconfigurados MVT. Esto es válido tanto en dispositivos Android, como en iPhone.

Recomendamos investigar estas opciones, experimentar con ellas y colaborar con el proyecto, ya que detrás de PiRogue Tool Suite hay hackers trabajando duro y desinteresadamente para que esta herramienta sea lo mas precisa y eficiente posible. En la propia página web se encuentra la documentación donde se explica paso a paso cómo utilizar la herramienta. Y, como siempre, recomendamos que los militantes con conocimientos técnicos configuren dispositivos de estos en casos de sospechas o si la situación dentro de un espacio militante lo requiere. También rogamos que si alguna vez alguien sabe que le han instalado un spyware en su dispositivo, se ponga en contacto con nuestro colectivo para que recojamos toda la información posible sobre el funcionamiento del programa espía, con el objetivo de generar indicadores que sirvan a las organizaciones para detectar estos programas.

Conclusiones

A modo de resumen, hemos visto cómo la presencia cada vez mayor de la tecnología en nuestras vidas, en este caso el smartphone que llevamos a todos los lados, supone un peligro para la seguridad en la militancia revolucionaria. El smartphone facilita nuestra localización, facilita que se escuchen y se lean nuestras conversaciones, que se sepa con quién hablamos y con qué frecuencia y, finalmente y en general, que se acceda a información que deberíamos ocultar. Es un problema muy grande para la militancia, sobre todo porque, pese a todos sus peligros, es una tecnología útil que utilizamos en el día a día, de la que frecuentemente no podemos prescindir, que facilita estar informados y comunicados y que, en muchos casos, también facilita realizar tareas militantes. Por ello y siguiendo la tónica habitual en estos temas sobre seguridad informática en la militancia, tenemos que medir bien en qué casos usar el smartphone, cuánto usarlo y cómo lo usamos.

A continuación, resumimos las ideas clave para gestionar de forma segura el uso del smartphone en el ámbito militante:

- No llevar el smartphone ni ningún dispositivo electrónico con conexión a cualquier tipo de red a manifestaciones, reuniones, eventos o cualquier otro tipo de actividades militantes. Si se lleva porque no queda otra, que esté apagado en todo momento, desde que se está lejos del lugar de encuentro hasta alejarse de nuevo de esa zona.
- Nunca hablar ni almacenar información comprometida o secreta en el dispositivo móvil. Si se hace, borrarla tan

pronto como haya cumplido su función. Usar códigos secretos, jerga o modos de expresión que dificulten a terceros entender de qué se está hablando.

- No hablar nada relacionado con información comprometida en presencia de un smartphone o de cualquier dispositivo electrónico.
- Las comunicaciones siempre por chat cifrado o por llamadas cifradas. Nunca usar aplicaciones de mensajería sin cifrado o de empresas privadas. Nunca usar el SMS ni las llamadas telefónicas normales. Priorizar software de mensajería instantánea que no identifique a las personas y que utilice nombres de usuario.
- No guardar los números de teléfono de nuestros compañeros. No identificar los nombres de usuario u otro tipo de cuentas con los nombres reales de las personas que están detrás.
- El GPS no es la única forma de geolocalizar un dispositivo. La red móvil es más útil para ello. De nuevo, no llevar el smartphone a actividades comprometidas.
- Si nos detienen y requisan nuestro dispositivo móvil, no volver a usarlo. Lo mismo ante cualquier indicio de que la policía haya podido acceder físicamente a él.
- Si creemos que hemos sido infectados por spyware, de forma física o remota, deshacernos del dispositivo.
- Si notamos que nos siguen, que vamos a ser detenidos o que pueden hacernos una redada, apagar el smartphone lo antes posible, para dejarlo cifrado.

- Cifrar el móvil, si no lo está ya.
- Para aquellos que puedan permitírselo, comprar un Google Pixel e instalarle GrapheneOS.

Para todo lo demás, se puede utilizar el smartphone. Son muchos los puntos, pero realmente se reducen a una idea:

- **El smartphone es un potencial espía de nuestras conversaciones, de los lugares en los que estamos y de la gente con la que nos relacionamos; actúa como si esa potencialidad fuese una realidad.**

La solución a la seguridad en los smartphone no está escrita, sino que consiste en un gran cúmulo de conocimientos muy difíciles de sintetizar y de hacerlos accesibles a la militancia sin conocimientos técnicos. Por eso, hacemos un llamamiento para que acudáis a vuestro hacklab más cercano o que preguntéis a vuestros compañeros con conocimientos, para informaros y aprender a diseñar estrategias de seguridad, ya que lo más importante es tener una buena lógica o estrategia de seguridad, más que conocimiento técnico exacto de cada tecnología.