VIGILANDO A LOS VIGILANTES

UNA GUÍA PARA CUIDARNOS DE ESTRATEGIAS BASADAS EN LA TECNOLOGÍA PARA MONITOREAR, INTIMIDAR O SILENCIAR NUESTRO ACTIVISMO

LAS REDES Y LAS CALLES: NUESTROS CAMPOS DE LUCHA

La internet y las calles son espacios de disputa. Allí nos encontramos para luchar por las causas que defendemos, y también resistimos en contra de grupos que por medio del acoso y la vigilancia, buscan silenciar nuestras voces y bloquear los cambios que buscamos o necesitamos. ¿Sabías que la Policía Nacional del Perú podría ser uno de los grupos que nos vigila?

Pero no temas. No todo está perdido. En esta guía encontrarás una serie de recomendaciones y aclaraciones para seguir realizando activismo de manera segura. Comparte esta guía, sobre todo, con aquellas personas que realizan activismo en situaciones de riesgo por defender sus cuerpos, identidades y territorios.
¡Vigilemos a los que nos vigilan!

EL DERECHO A EXPRESARNOS CON SEGURIDAD Y SIN REPRESIÓN

La Constitución Política del Perú, los tratados internacionales ratificados por el Estado peruano, las leyes, y las normas reglamentarias[1] que protegen nuestros derechos en internet y en los espacios públicos.

El Estado peruano tiene la obligación internacional de respetar, garantizar y adoptar la normativa para hacer efectivos nuestros derechos a:

1. La protección de la honra y la dignidad
2. La protección de la ley contra injerencias arbitrarias o ataques a nuestra vida privada, familia, domicilio o correspondencia
3. La libertad de expresión, de modo que “nadie podrá ser molestado a causa de sus opiniones” ni podrá ver restringido su derecho “por vías o medios indirectos encaminados a impedir la comunicación y la circulación de ideas y opiniones”.

En nuestro Derecho interno, la Constitución peruana también prohíbe la persecución por razón de ideas, reconoce el derecho a las libertades de información, opinión, expresión y difusión del pensamiento, y protege los derechos a la intimidad personal y al secreto e inviolabilidad de las comunicaciones y documentos privados[2].

[1] Ley de la Policía Nacional del Perú (DL 1267), art. 25.
[2] Constitución Política, arts. 2.3, 2.7 y 2.8.

ESTRATEGIAS PARA SILENCIARNOS

Un agente policial podría utilizar diversas conductas, basadas en el uso de la tecnología o de la fuerza, para monitorear, vigilar o acechar a personas que realizamos activismo. Esto nos puede generar angustia, pero recuerda que existen diversas estrategias para cuidarnos de cualquier intento de represión o censura. Conozcamos cada una de estas conductas y qué dice la Ley peruana sobre ellas.

EN LAS REDES

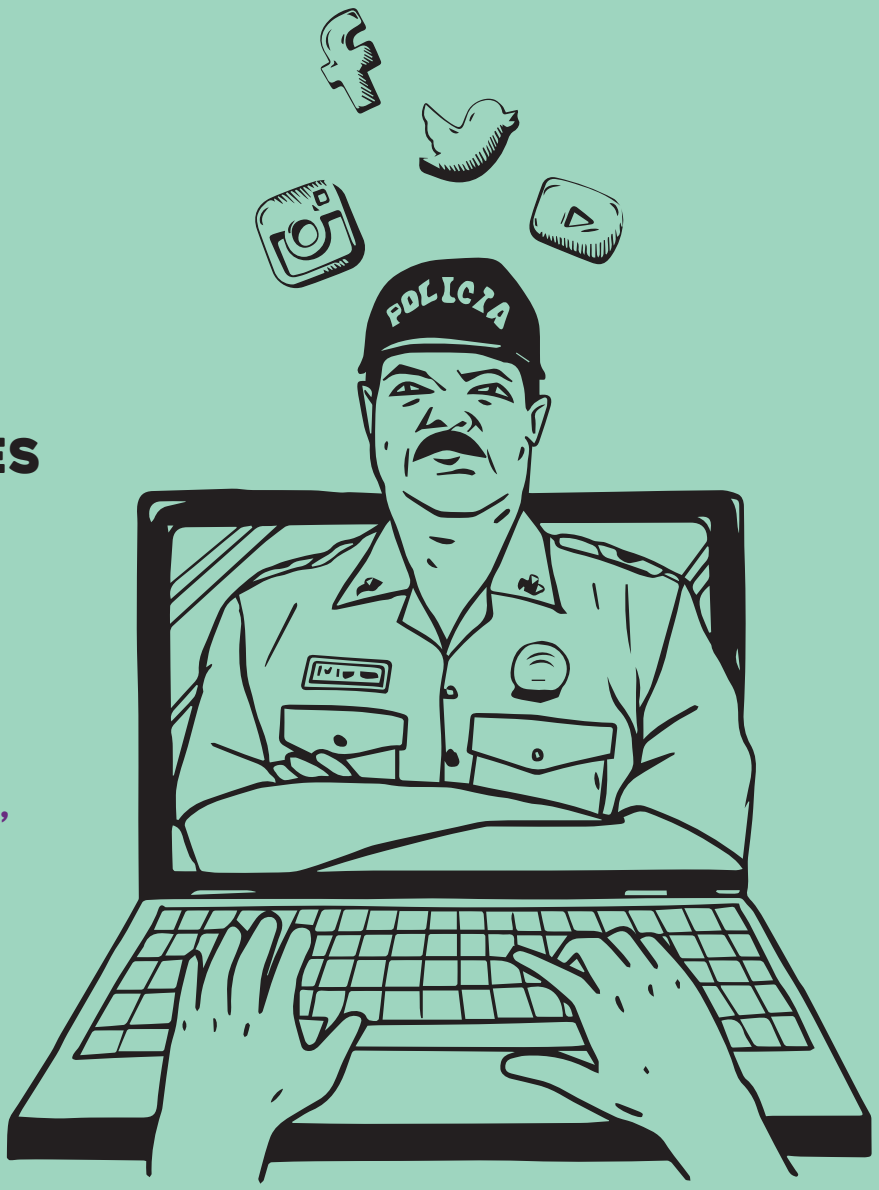
EN LAS CALLES

EN LAS REDES

1. MONITOREO DE REDES SOCIALES

¿Nuestras redes, nuestras reglas?

El monitoreo por medio de redes sociales consiste en que un agente visite perfiles públicos o privados, para recabar información. Al hacerlo, podría recopilar nombres de activistas, sus lugares de reunión y sus planes de movilización.



¿La Policía tiene la tecnología para monitorearnos? Sí. Para hacerlo, no necesitan tecnología sofisticada. Cualquier persona con acceso a Internet puede hacer este trabajo y únicamente necesita conocer bien las plataformas donde desea buscar información.

¿Qué información podrían captar? Existe mucha información en Internet sobre nosotros que incluso no sabemos que está ahí. En muchos casos, es información que hemos subido o que ha sido publicada por personas cercanas. Si realizamos una búsqueda rápida de nuestro nombre en un navegador, sería posible encontrar las redes sociales en las que tenemos una cuenta, así como fotos e información sobre nuestras amistades, colegas, lugares que visitamos, etc.

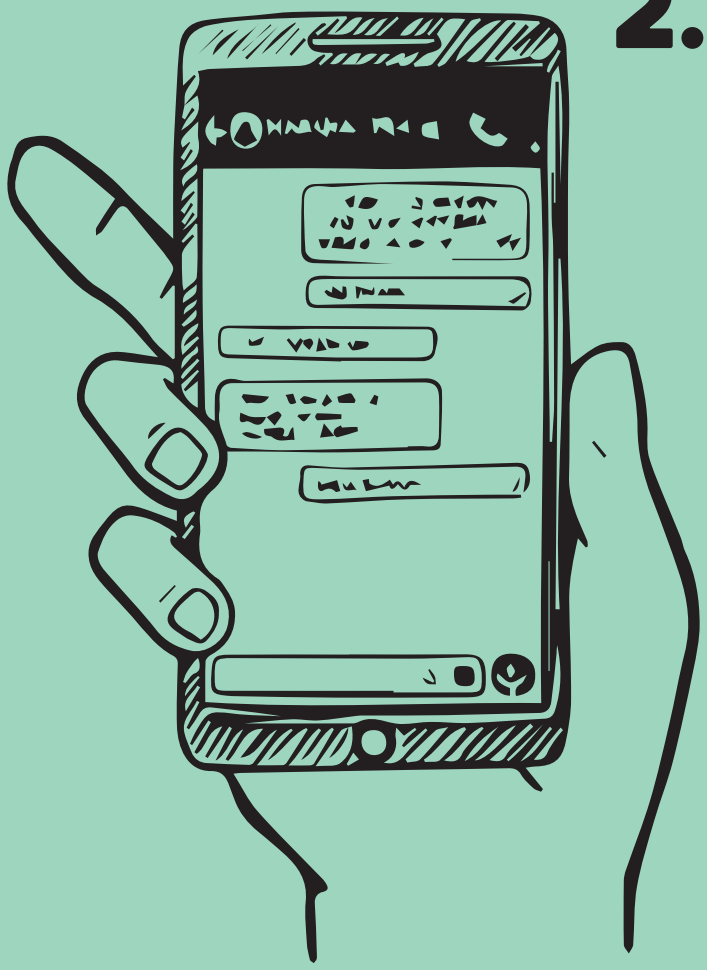
¿Es legal? Sí. La Policía Nacional, con o sin una investigación iniciada contra una persona, sí puede emplear los sistemas de **patrullaje virtual**[3] para la detección de delitos cometidos por medio de las tecnologías de la información y comunicación, los sistemas de información y comunicación policial, entre otros. Eso significa que la Policía puede monitorear la actividad en línea —tan igual como sucede con las cámaras de videovigilancia en vías y espacios públicos—, siempre y cuando lo haga en el marco del respeto a los

derechos fundamentales de las personas. Sin embargo, a la fecha no hay protocolos sobre patrullaje virtual que sean públicos a la ciudadanía.

¿Cómo me cuido? Recuerda que tu información pública la podrán ver todas las personas que puedan acceder a tu perfil en redes sociales. Configura tu privacidad para evitar que desconocidos tengan acceso a información como tu celular, tu dirección o lugar de estudios.

Además, cada vez que uses una aplicación o una web, brinda únicamente la información necesaria para su uso. Otra opción también es que utilices otro correo, cuenta o seudónimos para cuentas con fines de activismo.

[3]Ley de la Policía Nacional del Perú (DL 1267), arts. 25, 43



2. INFILTRACIÓN EN CANALES DE COMUNICACIÓN

Nos leen sin invitación

Un paso más allá del monitoreo es la infiltración en las comunicaciones (grupos de mensajería o grupos cerrados en redes sociales) de activistas para darle seguimiento a sus actividades y a información más sensible. Esto les permitiría identificar sus contactos, planes o espacios de encuentro.

¿La Policía tiene tecnología para infiltrarse en mis conversaciones?
Al igual que en el caso anterior, no necesita tecnología sofisticada. Solo necesita del anonimato.
En el caso de redes sociales, basta con crear una cuenta falsa y solicitar acceso a un grupo.
De hecho, es posible crear muchas cuentas falsas con nombres y correos electrónicos diferentes, así sean manejadas por la misma persona. En el caso de un grupo de mensajería, si quisieran
infiltrarse tendrían que revelar su número de teléfono. Sin embargo, existen grupos con tantos miembros que no siempre verificamos la identidad de todas las personas integrantes. Además, algunas aplicaciones brindan la opción de ocultar el número para quienes no estén en la lista de
contactos, lo cual dificulta el proceso de verificación. No olvides verificar a todos los integrantes de tus grupos.

¿Es legal? En principio, no hay una prohibición específica, ni para las personas en general ni para los policías en particular, de hacer uso del anonimato en redes sociales. En ese sentido, si ingresan a tus grupos sin cometer ningún delito (por ejemplo, suplantación de identidad), sino utilizando las propias reglas de Internet, se trata de una actuación legal. Sin embargo, cuando se trate de agentes encubiertos que participen de la realidad social y legal bajo una identidad supuesta (que incluye Internet), tendrán que contar con autorización del fiscal en el marco de una investigación específica.

¿En qué situaciones sí está permitida la actuación de un agente encubierto?
El fiscal puede disponer la autorización de agentes encubiertos cuando se trate de la investigación de delitos

informáticos, delitos de la criminalidad organizada, trata de personas, delitos de contra la administración pública y de **todo delito que se cometa mediante tecnologías de la información o de la comunicación**[4], incluso si no están vinculados a una organización criminal. Esto expone a activistas y defensores de derechos humanos a la posible criminalización de sus actividades.

¿Una persona infiltrada en mi grupo de mensajería es lo mismo que un terna (agentes encubiertos en protestas)? No.
Los miembros del Grupo Terna[5] no son los mismos agentes que realizan patrullaje virtual (que pertenecen a la Divindat) ni los que actúan como agentes encubiertos en delitos específicos (incluyendo delitos cometidos mediante las TIC). Es importante saber diferenciarlos en caso tengas que hacer una denuncia.
Si identificas a un agente policial infiltrado en tus grupos de mensajería, puede tratarse de un agente encubierto.

¿Qué hago si identifico a un agente policial infiltrado en mi mensajería? Lo ideal sería eliminarlo del grupo si tienes la capacidad de hacerlo o notificar a lxs administradorxs. Inmediatamente comprueba si este agente es parte de otros grupos de comunicación del que eres parte. En lo posible, utiliza aplicaciones de mensajería (como Telegram o Signal) que te den la posibilidad de no mostrar tu nombre y número de teléfono para las personas que no son nuestros contactos.

---

[4]Ley de la Policía Nacional del Perú (DL 1267), arts. 25, 43

[5]El Grupo de Inteligencia Táctica Operativa Urbana, conocido como "Grupo Terna", es una unidad especializada de la División de Operaciones Especiales y Jóvenes en Riesgo – Escuadrón Verde de la Policía Nacional del Perú. Su objetivo es realizar intervenciones policiales en "puntos críticos" de alta incidencia delictiva para la lucha contra la delincuencia común.

3. INTERCEPTACIÓN DE LLAMADAS TELEFÓNICAS
Mis llamadas no son un podcast

Otra manera de recabar información sensible es por medio de la interceptación de nuestras llamadas o de nuestros celulares. Es más complejo que la infiltración y sería un mecanismo efectivo para escuchar nuestras conversaciones privadas.

¿La Policía tiene la tecnología para interceptar llamadas? No existe evidencia de que la Policía tenga la tecnología adecuada para interceptar llamadas. Debemos diferenciar las llamadas telefónicas tradicionales con las llamadas a través de Internet mediante aplicaciones como WhatsApp, por ejemplo. Por un lado, las llamadas tradicionales son grabadas y almacenadas por las compañías de telefonía, y en algún momento pueden ser recogidas haciendo uso del levantamiento de secreto de las comunicaciones. Por otro lado, las llamadas a través de aplicaciones no quedan grabadas, aunque esto no significa que otros datos como la hora de inicio y fin de la llamada no pueden ser almacenados en los servidores de la empresa que provee el servicio.

¿Es legal que un agente intercepte las comunicaciones de personas activistas?[6] El secreto de las comunicaciones, al ser un derecho protegido por la Constitución, solo puede ser levantado en situaciones específicas, cuando la persona sea investigada por un delito cuya pena sea superior a cuatro años de privación de la libertad[7]. Para que exista una orden judicial que lo autorice, debe haberse iniciado una investigación preliminar o jurisdiccional. Además, la resolución judicial que autorice la interceptación debe indicar el nombre y, de ser posible, la identidad del teléfono o medio a intervenir, grabar o

[6]Constitución Política del Perú, art. 2.10; Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional (Ley 27697), art. 1; Código Procesal Constitucional, art. 230

[7]Código Procesal Penal, art. 230, numerales 1 y 2.

registrar, además de la forma de interceptación, alcance, duración, y dependencia policial o fiscal encargada. Cualquier interceptación de las comunicaciones que no haya sido autorizada mediante orden judicial es ilícita.

¿Puedo identificar si un agente policial está interceptando mis llamadas? Por el momento no existe una señal que nos permita confirmar que estamos siendo víctimas de interceptado de llamadas. Por eso, si encuentras que tu señal de teléfono se entrecorta o que pierdes señal, recuerda que estas no son características de la intercepción.

¿Cómo me cuido? La mejor estrategia para cuidarnos de la intercepción de llamadas es realizar llamadas solo desde aplicaciones de mensajería de comunicación encriptada como Whatsapp, Telegram (a través de los chats secretos) o Signal. Ningún actor externo, incluida la policía, podría acceder al contenido de una llamada de manera remota, si está encriptada de punto a punto.

4. OBTENCIÓN O FILTRACIÓN DE DATOS PERSONALES

Violentando mi privacidad

Una estrategia de intimidación común es obtener y filtrar los datos personales de quienes han participado en marchas o protestas. El efecto es lograr que se sientan vigiladas o perseguidas.

¿La policía tiene acceso a mis datos personales? La RENIEC maneja una base de datos principal, el Registro Único de Identificación de Personas Naturales, que contiene, entre otros, número de DNI, nombres y apellidos, fecha de nacimiento, estado civil, dirección y domicilio declarado, e, incluso, la firma de la persona. Normalmente, las entidades públicas pueden acceder al servicio de consultar en línea dicha base de datos haciendo un pago; sin embargo, RENIEC tiene más de un convenio con el Ministerio

del Interior para facilitar a la PNP el acceso a esta base de datos de manera gratuita, además de otros servicios.

¿Hay límites sobre lo que la Policía puede hacer con mis datos personales? La PNP debe guardar estricta reserva de toda información o datos a los que tenga acceso, y está prohibida de utilizarlos para fines distintos a sus funciones. Asimismo, la PNP puede recoger datos personales, conforme a la Ley y Reglamento de Protección de Datos Personales. Según dicha normativa, la PNP podría manejar bases de datos, las cuales debe registrar ante la Autoridad de Protección de Datos Personales. A la fecha ninguno de los bancos registrados por la PNP recogen números telefónicos, aunque podría deberse a que existan bancos sin registrar que sean de uso de la PNP[8].

¿La Policía podría estar utilizando tecnologías más sofisticadas para acceder a mis datos? No necesariamente. Existen mecanismos más sencillos para obtener esta información. Por ejemplo, en el marco de una protesta, mucha actividad y coordinaciones se realizaron a partir del uso de redes sociales o aplicaciones de mensajería. Esto implica que la información de los responsables de estas coordinaciones se puede filtrar, poniendo en riesgo información personal que le permitiría a un agente policial, o a cualquier persona, identificarnos. Esta información incluye nuestra dirección o número telefónico.

Entonces, si la Policía logra acceso a mi número telefónico, ¿ya me puede identificar? En el Perú, la adquisición de un chip de cualquier operador de telefonía requiere una identificación y validación biométrica. Esto implica que cada chip está asociado a una persona. Otra vulnerabilidad que puede ser aprovechada es la información que obtienen las aplicaciones de billetera digital que siempre solicitan un número de celular para asociarlo a la cuenta.
Este tipo de situaciones hacen muy sencillo que un policía pueda tener acceso a mayor información a partir de nuestro número de teléfono.

¿Existen otras maneras para obtener mis datos personales? Sí. Además de encontrar esta información en redes sociales, las filtraciones de datos personales son, lamentablemente, muy comunes. Existen muchas páginas web y aplicaciones que nos permiten realizar la búsqueda de datos personales de los peruanos. Esto se debe a que muchas páginas web del gobierno son obsoletas y antiguas o no tienen la seguridad requerida que evita que otras personas puedan hacer búsquedas o acceder a información personal de manera sencilla.

¿Qué hago si descubro que mis datos personales han sido filtrados u obtenidos de manera ilícita por un agente policial? Si se trata de la recopilación ilícita de datos personales por parte de la PNP como institución, podrías denunciarlo ante la Autoridad Nacional de Protección de Datos Personales para que inicien un procedimiento sancionador. También podría tratarse de un delito cometido por un agente policial (por ejemplo, uso indebido de archivos computarizados o tráfico ilegal de datos), con agravante por el abuso de una posición especial en razón del ejercicio de un cargo o función, lo cual es denunciable ante el Ministerio Público.

[8]Reglamento de la Ley de Protección de Datos Personales (DS 003-2013-JUS), art. 76.

5. INFORMACIÓN FALSA Y DESPRESTIGIO

El ataque a nuestra reputación

En el espacio digital, la información falsa se puede viralizar y llegar a miles de personas en cuestión de segundos. Una estrategia de desprestigio buscaría deslegitimar y debilitar el accionar activista y finalmente silenciar a quienes buscan levantar sus voces en internet y en las calles.

¿Un agente policial puede circular imágenes o información falsa sobre mí? Si un efectivo de la PNP, o cualquier otra persona, busca incriminar a alguien difundiendo contenido difamatorio, comete un delito contra el honor. Toda persona que atribuya a alguien, de una manera en la que pueda difundirse, la realización de un hecho o conducta que pueda perjudicar su honor o reputación, comete el delito de difamación[9], con circunstancia agravante si el sujeto activo fuera un miembro de la Policía Nacional[10]. Este delito también puede tener lugar a través de medios virtuales, como blogs o redes sociales.

¿Qué puedo hacer si identifico que circulan imágenes o información falsa sobre mí? De manera inmediata podrías comprobar qué información personal sobre ti está en Internet y cómo un adversario puede utilizarla para atacarte de manera física o virtual. Recuerda que ante las noticias falsas es recomendable interactuar lo menos posible con su contenido. Al responder, o compartir esta información, incluso para desmentirla, estamos apoyando que se difunda más. Siempre tenemos la opción de denunciar o reportar el contenido que han implementado muchas plataformas. De manera alternativa puedes optar por crear un registro de estos incidentes, guardarlos en páginas como archive.today, y presentar ese contenido como evidencia para hacer una denuncia por el delito correspondiente (por ejemplo, suplantación de identidad, si correspondiera) ante el Ministerio Público, o una querella ante el Poder Judicial (por ejemplo, por difamación)[11].

---

[9]Código Penal, art. 132.

[10] Código Penal, art. 46.

[11]Los delitos tipificados en el Código Penal y otros cuerpos normativos (como la Ley de Delitos Informáticos) pueden ser de persecución pública o privada. Cuando son de persecución pública, el Ministerio Público está a cargo de la investigación y representación del agraviado. Cuando son de persecución privada, en cambio, como sucede contra los delitos contra el honor (injuria, difamación, y calumnia), es la persona afectada quien debe procurarse un abogado y presentar una querella ante el Poder Judicial.

EN LAS CALLES

6. BLOQUEO DE SEÑAL
Cuando la red falla

Al salir a la calles durante una manifestación, es posible que perdamos la señal y ya no podamos comunicarnos con nuestros compañeros y compañeras. ¿Esta es una estrategia para bloquearmi activismo? Aquí te contaremos la razón por la cual esto sucede.

¿Es posible bloquear la señal durante una protesta? Tecnológicamente, es posible generar ruido electromagnético con el fin de bloquear las señales de las antenas de telecomunicaciones. Su uso más común en Perú es en las cárceles; sin embargo, también ha sido utilizado en otros países para prevenir la comunicación durante exámenes y así evitar la comunicación entre los alumnos. Potencialmente, se podría utilizar para bloquear la comunicaciones en una protesta; aunque, por el momento, no existe evidencia de que la Policía haya utilizado algún tipo de bloqueador de señales durante las protestas de Perú.

¿Es el único motivo por el que se puede perder la señal de los celulares? No, también es posible que, debido a una gran cantidad de personas concentradas en un mismo espacio, se genere una saturación en el servicio de telefonía, lo que produciría que las personas no puedan realizar llamadas, recibir mensajes o conectarse a Internet. Este tipo de problemas también se experimentan durante conciertos y eventos deportivos.

¿Es legal que bloqueen la señal durante una protesta? La producción deliberada de interferencias perjudiciales por parte de las empresas de telecomunicaciones constituye una infracción muy grave[12]. Si es una persona la que está interfiriendo con el normal funcionamiento de los servicios de telecomunicaciones (por ejemplo, el de Internet), dicha conducta constituye un delito[13]. A la fecha, solo está regulada la operación de equipos bloqueadores o inhibidores de señales radioeléctricas en los establecimientos penitenciarios y centros juveniles de diagnóstico y rehabilitación[14].

¿Qué puedo hacer para no quedarme incomunicado ante un bloqueo? Al participar en eventos masivos, como protestas por ejemplo, debemos anticipar que este tipo de problemas puede ocurrir.
Tener un plan de contingencia para poder comunicarnos cuando esto ocurra. Una alternativa son las aplicaciones off-the grid que permiten comunicación por Bluetooth; sin embargo, su principal desventaja es que funcionan en un rango muy corto.

---

[12]Texto Único Ordenado de la Ley de Telecomunicaciones (DS 013-93-TCC), arts. 3 y 87.

[13] Dependiendo del contexto, puede tratarse del delito tipificado en el artículo 206, inciso 6, del Código Penal, daño agravado de un bien (por daño a la infraestructura o instalaciones de servicios de telecomunicaciones); artículo 283, entorpecimiento al funcionamiento de servicios públicos; o artículo 281, atentado contra la seguridad común (cuando, producto del daño de la infraestructura o instalaciones de telecomunicaciones,también se cree un peligro para la seguridad).

[14]DS 012-2012-MTC, art. 1; DS 007-2016-JUS, Segunda Disposición Complementaria.


PASION
ROJBLAN
PNP


JUSTICIA.
VICTIMAS

7. SUSTRACCIÓN O DAÑO DE DISPOSITIVOS

¡Ese celular es mío!

Durante una protesta, llevamos nuestros celulares y cámaras fotográficas para mantenernos en comunicación y registrar abusos policiales. Obtener acceso o destruir estos dispositivos puede ser un mecanismo para controlar la información que se encuentra dentro de ellos.

¿Es legal que un agente confisque o destruya mi dispositivo? Lo único que la Policía puede solicitar, de ordinario y sin necesidad de orden de un fiscal o juez, es el Documento Nacional de Identidad, frente a lo cual el intervenido tiene derecho a exigir que el policía también se identifique (nombre y dependencia). Sin embargo, para el registro e incautación de bienes (por ejemplo, celulares o cámaras fotográficas), se requiere de una disposición fiscal, o, cuando haya negativa a entregar el bien, una orden del Juez de Investigación Preparatoria. Eso significa que, sin una orden judicial, la policía no puede revisar tu celular o cámara fotográfica, ni mucho menos alterar su contenido (lo que constituye una falta muy grave).

¿En qué situaciones está permitido que registren mis bienes (incluyendo dispositivos) sin una disposición previa? Solo en casos de flagrante delito (o cuando existan fundadas razones para creer que el intervenido pueda estar vinculado a la comisión de un hecho delictuoso[15]), la Policía podrá registrar a una persona a fin de hallar el bien relacionado con el delito, luego de lo cual levantará un acta y dará cuenta al Fiscal[16]. La Policía debe indicar las razones de la intervención e invitar a la persona a exhibir y/o entregar el bien buscado.
Según el protocolo de registro, además, el personal policial debe documentar todo el procedimiento por el medio audiovisual más idóneo,

[15] A pesar de que la norma expresamente señala que la Policía puede hacer un registro personal sin orden fiscal cuando tenga fundadas razones de sospecha de un delito, ya hay pronunciamientos judiciales que consideran no es así, y que la Policía solo puede proceder sin disposición fiscal en casos de flagrancia o de peligro inminente de perpetración del delito. Ver: Corte Superior de Justicia de la Libertad, Tercera Sala Penal Superior, Expediente 1193-2014-42, párr. 16.[19] Código Penal, art. 210, inciso 4.

[16] Base legal: DL 1267, art. 3; Código Procesal Penal, arts. 68.1.c, 203.3, 205, 210, 218.2; Acuerdo Plenario 5-2010/CJ-116

siempre que sea posible. Recuerda que tienes el derecho de manifestarte, lo cual no constituye ni es indicio de la comisión de un delito.

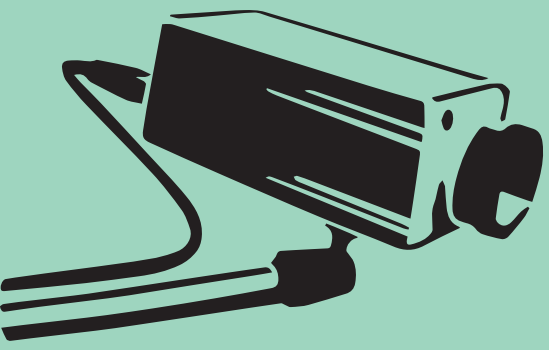
¿Qué puedo hacer para minimizar los daños ante una confiscación de mis dispositivos?

- Es altamente recomendable que nuestra información esté encriptada. Si tienes un celular Android, podrás cifrar toda la información que tienes almacenada en el dispositivo incluyendo tus datos personales, y tus imágenes.
- Desactivar la validación por huella dactilar o identificación facial antes de ir a una protesta. Utiliza únicamente el desbloqueo por contraseña. Si un agente policial te pide que le des tu contraseña, puedes negarte.
- Si vas a asistir a una manifestación y temes que puedan confiscar tus bienes, puedes tener presente el artículo 218 del Código Procesal Penal a fin de señalárselo verbalmente al efectivo policial, ya que solo podrían pedirte que entregues o exhibas un bien que sea cuerpo de un delito que ya se encuentra en investigación (por lo que requiere autorización del fiscal), o cuando se trate de flagrante delito. Si persiste en sustraer un dispositivo a pesar de no cumplirse con los requisitos para ello, podría tratarse de la comisión del delito de hurto de uso, con circunstancia agravante por ser miembro de la Policía Nacional, por lo que podrías denunciarlo. Asegúrate de pedirle al oficial que se identifique (nombre y dependencia), por si surge esa eventualidad.
- Procura estar en grupos o, al menos, con la compañía de una persona de tu confianza. Si la Policía te registra alegando flagrante delito, tienes derecho a hacerte asistir por una persona mayor de edad de tu confianza, quien también firmará el acta, y puede dar conformidad de su exactitud.
- Si la Policía llega a registrarte, exige que todo sea grabado por el personal policial, conforme indica la legislación actual, o, de lo contrario, procura que la persona que te acompaña lo haga.

[17] Protocolo de actuación interinstitucional para la aplicación del registro y recepción, aprobado por Decreto Supremo N° 010-2018-JUS. Enlace: https://portal.mpfn.gob.pe/descargas/ncpp/files/c89543_PROTOCOLO%20DE%20ACTUACION%20INTERINSTITUCIONAL%20PARA%20LA%20APLICACION%20DEL%20REGISTRO%20Y%20RECEPCION-ilovepdf-compressed.pdf

[18] Código Penal, arts. 187, 46.

[19] Código Penal, art. 210, inciso 4.



8. CÁMARAS EN ESPACIOS PÚBLICOS
¡Te estoy viendo!

Cuando estamos en un espacio público, es posible que nos tomen fotos o videos sin nuestra autorización. En el caso de las fuerzas del orden, cuentan con varios dispositivos para tomar un registro de quienes están en una protesta desde un celular hasta una cámara de vigilancia.

¿La Policía está autorizada para realizar este tipo de vigilancia? Sí. Siempre que resulte indispensable para cumplir los fines de esclarecimiento, el Fiscal puede disponer que: (i) se realicen tomas fotográficas y registro de imágenes; y, (ii) se utilicen otros medios técnicos especiales determinados con finalidades de observación o para la investigación del lugar de residencia del investigado[20]. No obstante, si se requiriera que estos medios técnicos especiales se utilicen dentro de un inmueble o lugar cerrado, sí se necesitaría de una orden judicial. En ese sentido, si se registran imágenes de la esfera privada sin cumplir con los requisitos que plantea la norma, podría configurarse el delito de violación de la intimidad, con agravante por razón de función pública.

[20] Código Procesal Penal, art. 207.

Entonces, ¿una persona de las fuerzas del orden me puede tomar fotos en una protesta? En una protesta o manifestación, la Policía está cumpliendo un rol preventivo. Eso significa que deben garantizar que las personas puedan ejercer su derecho a la libertad de expresión, así como mantener el orden interno. Si bien sí pueden capturar fotografías de las personas, al tratarse de un espacio público, la Policía debe restringir el registro de imágenes para el esclarecimiento o investigación de un delito ya haya sucedido, y no para situaciones de protestas.

¿Se pueden utilizar cámaras de seguridad para vigilar a los activistas? Cámaras de videovigilancia están distribuidas en todos los distritos de la capital y son monitoreadas desde una central de información. En algunos casos, algunas dicen tener la tecnología de reconocimiento facial; sin embargo, no existe evidencia de que realicen esa validación y menos que se aproveche esta tecnología para hacer seguimiento a activistas. Sin embargo, debemos estar alerta. Las técnicas de reconocimiento facial en Perú están siendo utilizadas únicamente para las aplicaciones desarrolladas por RENIEC y su uso es netamente para agilizar procesos que antes eran presenciales. Esto confirma que existe un registro biométrico facial de la población peruana y que, potencialmente, puede utilizarse por las cámaras y la Policía Nacional.

¿Qué hago si identifico que me pueden estar vigilando? Usa mascarilla o vestimenta que tape tu rostro. La tecnología que usan las cámaras en Perú no cubren la identificación cuando las personas tienen las mascarillas puestas. Otra opción muy creativa utilizada en Corea fue utilizar apuntadores láser a los lentes de las cámaras en protestas. Esto no significa que se malograrán, pero su enfoque no funcionará como debe.


POLICIA
POLICIA
POLICIA
POLICIA
POLICIA


FILA

9. ACECHO Y SEGUIMIENTO
Cuando se sienten los pasos

Si una persona que nos quiere hacer daño obtiene nuestra dirección domiciliaria o lugar de trabajo, podría llevar a un seguimiento en lugares físicos dejando de lado el espacio virtual.

¿La Policía está autorizada para realizar este tipo de seguimiento? La Policía Nacional del Perú sí se encuentra facultada a realizar seguimiento y vigilancia de las personas. Para ello, debe contar con la disposición fiscal, sea de oficio o a pedido de la Policía, en el marco de una investigación por delitos violentos, graves, o contra organizaciones delictivas (es decir, no puede haber seguimiento y vigilancia policial a personas que no son sospechosas de algún delito, ni cuando se trate de delitos comunes).

¿La Policía puede utilizar la tecnología para rastrear y seguirme? La Policía Nacional del Perú podría solicitar la geolocalización de un celular, aunque no se haya iniciado una investigación fiscal. Este procedimiento está a cargo de la División de Investigación de Delitos de Alta Tecnología. Para que proceda la solicitud de acceso a los datos de geolocalización, debe tratarse de (i) flagrante delito, o (ii) un delito cuya pena sea mayor a cuatro años de privación de libertad; además, se requerirá que (iii) el acceso a dichos datos sean necesarios para

la investigación. Solicitar la geolocalización de un activista únicamente por manifestarse implica un tipo de criminalización de la protesta, pues no habría cometido ningún delito.

No obstante, aún si se configura alguno de estos supuestos, las atribuciones de la PNP deben seguir el procedimiento establecido en la ley, incluyendo la puesta en conocimiento del Ministerio Público. Si algún efectivo policial altera, induce o interfiere en dicho procedimiento estaría incurriendo en la comisión de una infracción muy grave, según la Ley que regula el Régimen Disciplinario de la Policía Nacional del Perú, y sería pasible de sanción al haberse configurado responsabilidad administrativa.

¿Esta es la única manera de rastrearme? No. La obtención de datos personales es otro mecanismo basado en la ingeniería social que podrían utilizarse para averiguar dónde vivimos o dónde nos reunimos para hacer activismo. Aunque no nos demos cuenta, mucha de nuestra información online puede dar pistas a los adversarios sobre los lugares que frecuentamos o vivimos. Por ejemplo, fotos o menciones a lugares como restaurantes o cafeterías.

¿Qué puedo hacer si creo que me están siguiendo? Si consideras que estás siendo seguido o que tu domicilio es vigilado de manera arbitraria o injustificada, puedes presentar una demanda de hábeas corpus ante Juez Penal (art. 25.13 del Código Procesal Constitucional).

Evitar hacer publicaciones sobre los lugares que frecuentamos o que sean fáciles de identificar por sus características. Otra recomendación es no hacerla mientras estemos en el lugar, sino luego o en otro día. De esta forma, evitamos el seguimiento.

Aunque es menos probable, es recomendable retirar el etiquetado GPS a las fotos que tomamos con la cámara del celular.

[21] Reglamento de la Ley de la Policía Nacional del Perú, art. 128
[22] Decreto Legislativo 1182, arts. 3 y 4
[23] Ley que regula el Régimen Disciplinario de la Policía Nacional del Perú (Ley 30714), tabla de infracciones y sanciones.


NUEVA
CONSTITU
POR Y

10. USO DE LA FUERZA
Exceso de fuerza, abuso de derecho

Recuerda que la violencia digital puede convertirse en violencia física. Si alguien obtiene tus datos personales, puede utilizarlos para seguirte, detenerte o ejercer violencia física. Sin embargo, recuerda que puedes protegerte.

¿Es legal que la Policía use la fuerza para detenerme? El uso de la fuerza de la PNP se sustenta en el respeto irrestricto a los derechos fundamentales. Eso significa que la fuerza se debe usar de manera progresiva y diferenciada, cuando sea estrictamente necesario, atendiendo a los niveles del uso de la fuerza normados.

Por otro lado, si un agente hace uso de la fuerza de manera innecesaria o desproporcionada en acto de servicio, ocasionando lesiones graves, comete una infracción muy grave (responsabilidad administrativa) y un delito (responsabilidad penal).

¿Qué puedo hacer si he sido víctima de una agresión policial física? Si esto sucede tienes dos vías: la penal y la administrativa. Por la primera de ellas, puedes presentar una denuncia por el delito de lesiones graves (o leves, de ser el caso). Sin embargo, hacer uso de la fuerza en forma innecesaria o desproporcionada ocasionando lesiones graves durante acto de servicio también es una infracción administrativa muy grave en el régimen disciplinario de la Policía Nacional. En ese sentido, puedes presentar una denuncia a través de la plataforma de Registro de Denuncias del Ministerio del Interior o escribir a inspector@pnp.gob.pe para recibir mayor orientación. También puedes realizar tu denuncia de manera escrita y presentarla ante la Inspectoría General de la PNP, encargada de efectuar las investigaciones administrativas disciplinarias en el ámbito de su competencia.

[24]Decreto Legislativo que regula el uso de la fuerza por parte de la Policía Nacional del Perú (DL 1186), arts. 7 y 8; Manual de Derechos Humanos Aplicados a la Función Policial (RM 952-2018-IN)

[25]Puedes revisar la tabla de infracciones y sanciones vigente en el siguiente enlace: http://spij.minjus.gob.pe/Graficos/Peru/2017/Diciembre/30/L-30714.pdf

[26]Reglamento del Decreto Legislativo Nº 1267, Ley de la Policía Nacional del Perú (aprobado por DS 026-2017-IN), art. 37.

GLOSARIO

Aprendamos sobre tecnología para que sea nuestra aliada y nos cuide de los vigilantes:

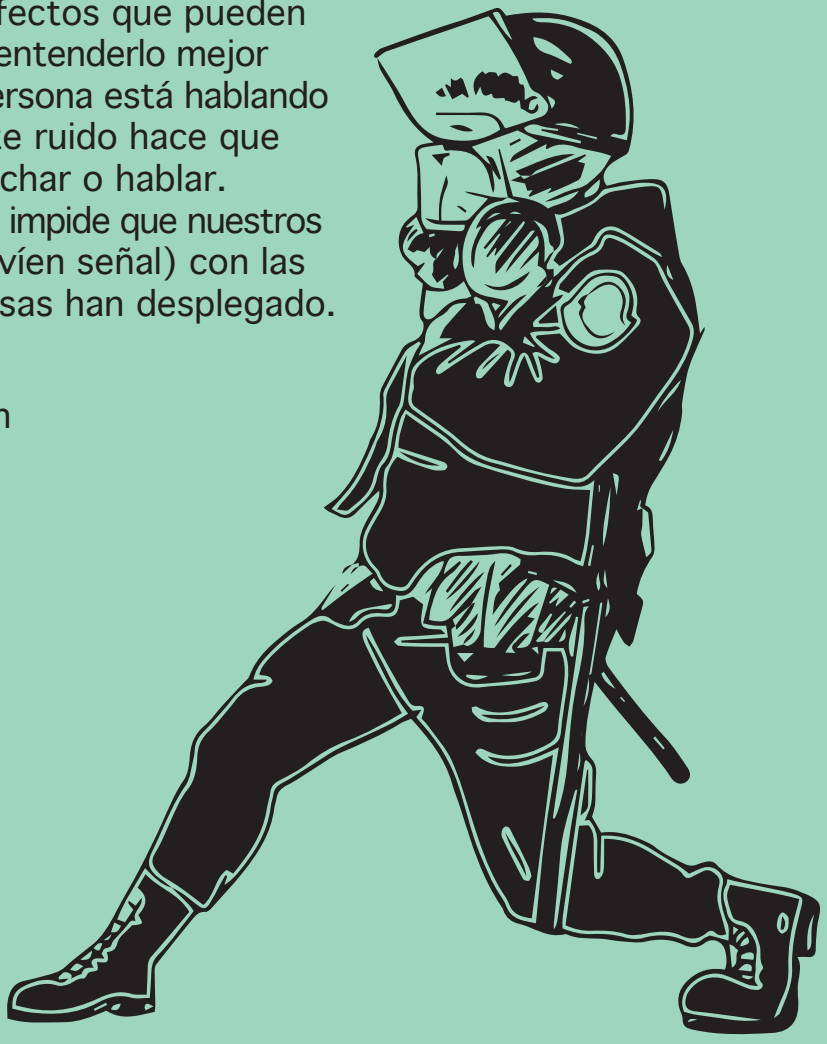
Detección facial: Es una tecnología que identifica el rostro de las personas. Esto es diferente al reconocimiento facial, ya que no lo asocia a una identidad, sino únicamente se enfoca en detectar si hay un rostro o no.

Encriptación: Es un proceso que utiliza métodos matemáticos para convertir los datos o información accesible en un código ininteligible que no puede ser leído o entendido por medios normales.

Reconocimiento facial: Es la tecnología con capacidad de identificar a una persona a través de una imágen o video haciendo uso de las características biométricas de su rostro.

Ruido electromagnético: El ruido eléctrico es una señal de interferencia eléctrica que se añade o se suma a nuestra señal principal (que puede ser nuestra señal de WiFi o señal de telefonía celular) de manera que la puede alterar produciendo efectos que pueden ser más o menos perjudiciales. Para entenderlo mejor podríamos asociarlo a cuando una persona está hablando muy fuerte al lado de nosotros. Este ruido hace que sea complicado para nosotros escuchar o hablar.
En el contexto de celulares, este ruido impide que nuestros smartphone “hablen” (reciban o envíen señal) con las antenas de telefonía que las empresas han desplegado.

Ingeniería social: La ingeniería social es una técnica de manipulación psicológica que utiliza el adversario para obtener información relevante sobre una persona. Muchas veces esta información es utilizada para cometer ciberdelitos como la suplantación de identidad o acceso no autorizado a cuentas. Este tipo de ataque no está limitado al espacio digital sino que también puede hacerse en persona. Es importante saber reconocer e identificar páginas seguras y verificables.



CONSEJOS GENERALES DE SEGURIDAD DIGITAL

Unos últimos consejos para llegar a las protestas preparades y segures:

ANTES DE IR A UNA PROTESTA

- Revisa la configuración de tus redes sociales. Responde preguntas como ¿quiénes pueden buscarme?, ¿quiénes pueden escribirme?, ¿quiénes pueden ver las fotos que subo?, ¿quiénes pueden etiquetarme en fotos? Adapta tus preferencias de privacidad para evitar que desconocidos o adversarios puedan ver tu información.
- Crea un perfil para tu activismo en redes sociales, independiente de tu perfil personal donde aparece información de tus familiares o colegas del trabajo.
- Utiliza contraseñas seguras y activa verificación de dos pasos para todas tus cuentas y perfiles.
- Cuando crees grupos de coordinación recuerda establecer reglas. Una regla, por ejemplo, es no compartir datos personales de coordinadores, información sensible o fotos de personas que no hayan dado consentimiento de que sus rostros sean publicados.
- Descarga aplicaciones que protejan tus datos y que te permitan comunicarte con encriptación de punto a punto.
- Desconfía de aplicaciones como los identificadores de llamada que piden acceso a nuestra lista de contactos o nuestro historial de llamadas.
- En muchos teléfonos con sistema operativo Android, el historial de tu recorrido se encuentra activo por defecto.
- Analiza si esa información es valiosa para ti o si alguien podría utilizarla para perjudicarte.

DURANTE UNA PROTESTA

- Lleva mascarillas, pañuelos o cualquier vestimenta que cubra tu rostro y cualquier rasgo identificable.
- Cuando subas fotos de otras personas, consulta con ellas si están de acuerdo en mostrar su rostro. O mejor aún, borra su rostro especialmente si están participando de una manifestación política.

- Evalúa si es necesario el etiquetado de GPS en las fotos tomadas desde el celular. Si lo vas a incluir, procura subir tus fotos de manera asincrónica (al día siguiente o cuando ya no estés en ese lugar).
- Lleva impresa información legal clave para evitar que un agente policial abuse de su poder.

DESPUÉS DE UNA PROTESTA

- Evita hacer clic en enlaces que te parezcan sospechosos o desconocidos y verifica si la dirección (URL) corresponde a la entidad que solicita tu información.
- Si te quitaron tu dispositivo, cambia todas tus contraseñas y revisa si han habido inicios de sesión desde lugares que tú no frecuentas. Si tenías activada verificación de dos pasos, te llegará una notificación cuando traten de acceder.
- Revisa si conoces a todas las personas que están participando en tus grupos de mensajería. Elimina a números desconocidos y no aceptes invitaciones de perfiles nuevos hasta que te sientas segura/o.
- Recuerda darte un tiempo para respirar y cuidar tu salud mental.

VIGILANTES, LOS ESTAMOS VIGILANDO

Ya no tenemos temor. Tenemos información y conocemos cómo protegernos del monitoreo y vigilancia policial injustificados. Ahora podremos activar de manera segura en las calles y en las redes. ¡No olvides compartir esta guía con tus amigues y compañeres!

Autores: HIPERDERECHO en colaboración con FAC FOTOGRAFXS AUTO CONVOCADXS

Diagramación e ilustraciones: Rocio Urtecho (Jugo Gástrico)

Fotografias: Archivo Fotografxs Autoconvocadxs

Gracias al apoyo del **Fondo de Respuesta Rápida 2021 de** PULSANTE CIDADANIA ATIVA