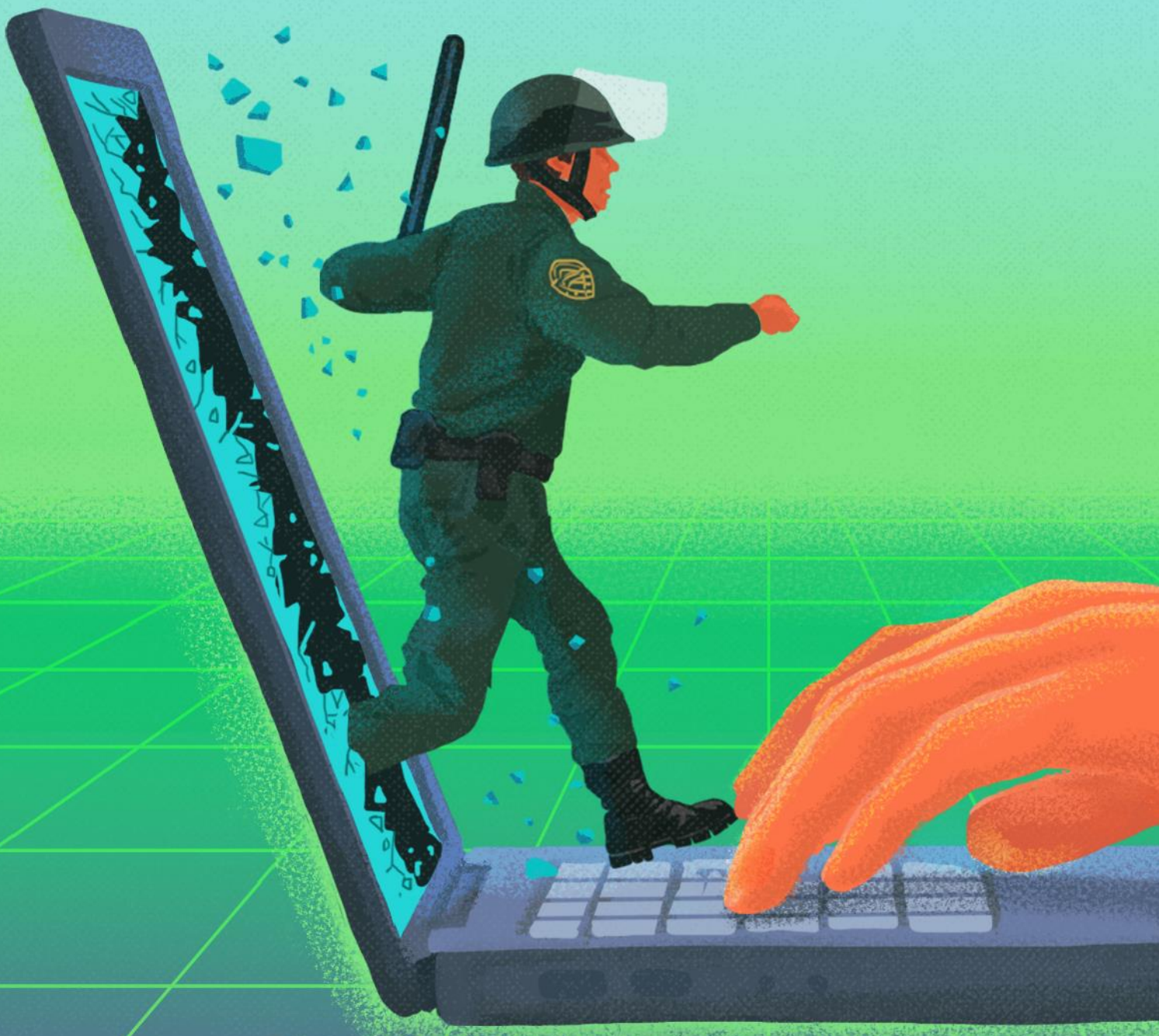
Informe de recomendaciones

Ciudadanía cuidando su derecho a la protesta ante el monitoreo a través de la tecnología



¿QUIÉN VIGILA A LOS VIGILANTES?

Un proyecto de

HIPER DERECHO
Tecnología como libertad

FAC FOTOGRAFXS AUTO CONVOCADXS

Introducción

La Internet y las calles son espacios de disputa. Allí se encuentra la ciudadanía para luchar por las causas que defienden, y también resisten en contra de grupos que por medio del acoso y la vigilancia buscan silenciar sus voces y bloquear los cambios que buscan o necesitan. Entre muchos, la Policía Nacional del Perú podría ser uno de los grupos que vigila a la ciudadanía mediante estrategias basadas en la tecnología.

Hiperderecho es una organización de sociedad civil que trabaja por la defensa y la promoción de los derechos fundamentales en línea y ha elaborado una serie de recomendaciones sobre cómo protegerse del monitoreo e intimidación policial frente al ejercicio del derecho a la protesta, en colaboración con el colectivo ciudadano Fotografxs Autoconvocadxs.

A partir de las protestas de noviembre del 2020 en Perú, recibimos una serie de consultas referentes a la vigilancia policial en espacios físicos y virtuales. Notamos que no existe o no se difunde información al respecto. En respuesta a esta necesidad, surge nuestro proyecto ¿Quién vigila a los vigilantes? En este, recolectamos una serie de testimonios de diversos activistas, quienes nos señalaron varios tipos de vigilancia que habían experimentado u observado. A partir de estas vivencias y dudas, hemos elaborado recomendaciones y aclaraciones acerca de los límites de la vigilancia policial en nuestro país.

Las cuestiones clave planteadas en este informe giran en torno a lo siguiente:

1. Tal como sucede en los espacios físicos, la Internet peruana es un espacio en el que los derechos son amenazados. Frente a ello, es necesario recordar que la Internet es nuestra. Por eso, las y los ciudadanos debemos **reapropiarnos de nuestros espacios digitales de manera segura y libre**. Para tal fin, sintetizamos algunas recomendaciones de seguridad digital que pueden ser útiles para aquellas personas que soliciten orientación y guía a su organización, así como para el propio uso de quienes integran su equipo.

2. Nuestros derechos y libertades deben poder ser ejercidos sin la intervención arbitraria de fuerzas del orden. Como señala la Convención Americana de Derechos Humanos, los Estados tienen la obligación de respetar (abstenerse de interferir en el ejercicio de los derechos ciudadanos), garantizar (el goce pleno de los derechos) y no discriminar (en el ejercicio de los derechos). Más allá de las competencias que les han sido asignadas, la Polícia Nacional del Perú está sometida a la Constitución Política del Perú, los tratados internacionales ratificados por el Estado peruano, las leyes, el Código Penal Militar Policial y las normas reglamentarias. Eso significa que nuestros derechos (en Internet y en espacios públicos) son el límite infranqueable e innegociable de sus actuaciones, salvo en casos excepcionales, que deben estar correctamente recogidos en la norma, y cuya interpretación es restrictiva. No obstante, **resulta preocupante que ciertos lineamientos y/o protocolos que guían algunas actividades policiales no sean públicas a la ciudadanía**, de modo que no es sencillo auditar si su contenido es conforme a la protección, respeto y garantía de nuestros derechos.

3. La protesta es un derecho fundamental. Como tal, la presencia de la Policía Nacional del Perú debería estar orientada a garantizar que pueda ejercerse de manera pacífica. Sin embargo, generalmente, es criminalizada. Muchas circunstancias en las que se pueden limitar derechos fundamentales (registro personal, levantamiento del secreto de las comunicaciones, seguimiento policial, etc.) requieren que se esté investigando un delito. **Al justificar que esos eventos sean utilizados contra activistas, dirigentes y ciudadanía en general (que, por su actividad, podrían ser considerados como defensores o defensoras de derechos humanos), se está criminalizando la protesta.**

En las redes

1. Monitoreo de redes sociales

La Policía Nacional puede emplear los sistemas de **patrullaje virtual**[1] 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 actividades en línea, independientemente de que haya un delito en investigación o no. Este monitoreo está a cargo del Departamento de Prevención y Patrullaje Virtual de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT). Sin embargo, a la fecha no hay protocolos sobre patrullaje virtual que sean públicos a la ciudadanía.

Recomendaciones

Es importante que las personas sepan cómo protegerse en línea. Por eso, si tienen la oportunidad, sugerimos que puedan recomendar a quienes requieran orientación que configuren su privacidad en redes sociales para evitar que desconocidos tengan acceso a información como celular, dirección o lugar de estudios. Otra opción es que se utilice otro correo, cuenta o seudónimos para cuentas con fines de activismo. A nivel de incidencia, invocamos a que puedan planificarse actividades que exijan transparencia a la Policía en cuanto a los protocolos que utilizan para este monitoreo, o que, en su defecto, los aprueben, con lineamientos respetuosos de los derechos fundamentales.

2. Infiltración en canales de comunicación

No existe una prohibición específica, ni para las personas en general ni para la policía en particular, de hacer uso del anonimato en redes sociales. Siempre que las personas ingresen a un grupo de mensajería sin cometer ningún delito (como el de suplantación de identidad), sino utilizando las propias reglas de Internet, se trata de una actuación legal. Un caso diferente es el de agentes encubiertos, a quienes se les asigna una identidad supuesta para que participen de la realidad social y legal (que incluye internet). Para ello, deben contar con autorización del fiscal en el marco de una investigación específica, sea por algún delito informático, delito de la criminalidad organizada, trata de personas, delito de contra la administración pública y o **cualquier delito que se cometa mediante tecnologías de la información o de la comunicación**[2]. Esto expone a activistas y defensores de derechos humanos a la posible criminalización de sus actividades.

Recomendaciones

Es recomendable tener controles de ingreso para los canales de comunicación grupales, y eliminar a aquellas personas que se logre identificar como infiltradas. Inmediatamente, se debería comprobar si esa persona es parte de otros grupos de comunicación del que se es parte. También sería ideal difundir la posibilidad de recurrir a algunas opciones de aplicaciones de mensajería como Telegram o Signal, que brindan la posibilidad de no mostrar nombre y número de teléfono para las personas que no están registradas como contactos. Por otro lado, es importante seguir concientizando sobre la naturaleza del derecho a defender derechos humanos, para que las personas no se sientan criminalizadas.

3. Interceptación de llamadas telefónicas

No existe evidencia de que la Policía tenga la tecnología adecuada para interceptar llamadas. En este punto, se deben diferenciar las llamadas telefónicas tradicionales con las llamadas a través de Internet mediante aplicaciones como WhatsApp, por ejemplo. Por un lado, las

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

[2] Ley de Delitos Informáticos (Ley 30096), Segunda Disposición Complementaria Final; Código Procesal Penal, art. 341

llamadas tradicionales son grabadas y almacenadas por las compañías de telefonía, que en algún momento pueden ser entregadas a los operadores de justicia haciendo uso del levantamiento de secreto de las comunicaciones, conforme lo establece nuestro ordenamiento jurídico: con orden judicial y cuando sea estrictamente necesario (es decir, que el Juez realice un test de proporcionalidad en el que encuentre que la medida del levantamiento del secreto de las comunicaciones es idónea, necesaria y proporcional). Por otro lado, el contenido de las llamadas a través de aplicaciones no quedan grabadas y almacenadas por parte de las empresas de telecomunicaciones (lo que no significa que otros datos, como la hora inicio y fin de la llamada, no pueden ser almacenados en los servidores de la empresa que provee el servicio).

Recomendaciones

Es muy importante que las personas reconozcan la ventaja de realizar llamadas únicamente desde aplicaciones de mensajería de **comunicación encriptada** como Whatsapp, Telegram (a través de los chats secretos) o Signal. Esto evitará que cualquier actor externo, incluida la policía, acceda al *contenido* de una llamada de manera remota, ya que estaría **encriptada de punto a punto.** Por otro lado, exhortamos a que puedan continuar en su trabajo de empoderar a la ciudadanía para que identifiquen la relevancia de su derecho al secreto de las comunicaciones, y reconozcan que solo en contextos específicos y excepcionales puede restringirse, previa orden judicial.

4. Obtención o filtración de datos personales

La PNP puede acceder al Registro Único de Identificación de Personas Naturales de Reniec de manera gratuita debido a los convenios interinstitucionales entre Reniec y el Ministerio del Interior. Asimismo, la PNP maneja varias bases de datos, entre las que se encuentran las del Sistema de Denuncias Policiales (Sidpol) y del sistema para el trámite del certificado de antecedentes policiales (en las cuales el número telefónico es de llenado opcional). Todos estos datos deben ser tratados respetando la Ley de Protección de Datos Personales y su Reglamento.

Fuera de estas bases de datos, existen otros mecanismos para acceder a datos personales. Por ejemplo, existen varias páginas web y aplicaciones que 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 evite que otras personas puedan hacer búsquedas o acceder a información personal de manera sencilla**.

Recomendaciones

Es momento de reflexionar sobre a quiénes entregamos nuestros datos personales (por ejemplo, billeteras digitales). Al crear cuentas, podemos facilitar que se obtengan más datos personales (por ejemplo, un nombre o cuenta bancaria asociados a un número telefónico). Por eso, es importante recordarle a la ciudadanía que presten atención a los datos y accesos que otorgan. Por otro lado, es importante visibilizar el riesgo que suponen las páginas web del gobierno que no cuentan con adecuados mecanismos de seguridad. Acciones de incidencia en este sentido pueden ser valiosas para nuestra sociedad.

5. Información falsa y desprestigio

Una estrategia para silenciar el activismo de las personas es difundir contenido difamatorio sobre ellas. Esas acciones en las que se busca incriminar a alguien, constituyen delito de difamación. Si el autor fuera un miembro de la Policía Nacional, además, se trataría de una circunstancia agravante[3]. Este delito también puede tener lugar a través de medios virtuales, como blogs o redes sociales.

[3] Código Penal, art. 46.

Recomendaciones

Si se identifica que circulan imágenes o información falsa sobre una persona, de manera inmediata se podría comprobar qué información personal existe en Internet y cómo un adversario puede utilizarla para atacar de manera física o virtual. Ante las noticias falsas es recomendable interactuar lo menos posible con su contenido. Al responder, o compartir esta información, incluso para desmentirla, se está apoyando que se difunda más. Siempre está la opción de denunciar o reportar contenido que han implementado muchas plataformas. De manera alternativa se puede 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).

En las calles

6. Bloqueo de señal

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.

También es posible que, debido a una gran cantidad de personas concentradas en un mismo espacio, se genera 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.

Recomendaciones

Es importante orientar a las personas para que mantengan la calma. Al participar en eventos masivos, como protestas por ejemplo, se debe anticipar que este tipo de problemas puede ocurrir. Es preferible tener un plan de contingencia para poder comunicarse 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. Por otro lado, desde la sociedad civil, es importante que sigamos vigilantes de las normas que regulen la operación de equipos bloqueadores o inhibidores de señales radioeléctricas, pues a la fecha solo están permitidos en los **establecimientos penitenciarios y centros juveniles de diagnóstico y rehabilitación**[4].

7. Sustracción o daño de dispositivos

Una preocupación relevante de dirigentes y activistas es qué puede pasar con sus bienes y dispositivos si son intervenidos. Aunque la ley señala que para el registro e incautación de bienes (por ejemplo, celulares o cámaras fotográficas) se requiere de una disposición fiscal, también prevé la posibilidad de que la PNP, 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), pueda hacer el registro[5]. Sin embargo, no hay criterios sobre cuáles podrían considerarse “fundadas razones”, en especial, en el marco de una protesta[6].

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

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

[6] 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

Recomendaciones

Para proteger los dispositivos, es altamente recomendable que la información **esté encriptada**. Si se cuenta con un celular Android, se podrá cifrar toda la información almacenada en el dispositivo incluyendo datos personales e imágenes. Asimismo, lo ideal sería desactivar la validación por huella dactilar o identificación facial antes de ir a una protesta, y utilizar únicamente el desbloqueo por contraseña, sin entregársela a la Policía si se lo solicitan.

Asimismo, **creemos que desde sus plataformas pueden realizar sugerencias en esta materia para que las personas sepan qué esperar de una intervención policial en estos contextos, y qué circunstancias deberían tener en cuenta para protegerse**. Desde nuestro proyecto, hemos invitado a que las personas se aseguren de que el efectivo policial se identifique, que estén en grupos o al menos con la compañía de una persona de confianza que también pueda firmar el acta, y que exijan que el personal policial graben el registro, conforme indica el protocolo actual[7]. No obstante, estamos seguros de que la experiencia que su organización tiene puede ser de mayor impacto para hacer pedagogía pública sobre los derechos de las personas frente a intervenciones de la PNP.

8. Cámaras en espacios públicos

Las 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, es necesario 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.

Recomendaciones

Hay diferencias entre las cámaras en espacios públicos y el registro de imágenes que puede realizar la Fiscalía en la investigación de un delito. Al respecto, recomendamos que se haga esa precisión ante posibles consultas de la ciudadanía, debido a que los medios técnicos especiales, como las tomas fotográficas, requieren de disposición fiscal y/u orden judicial, de ser el caso. En ese sentido, es importante seguir concientizando sobre la no criminalización de la defensa de los derechos humanos. Por otro lado, para protegerse de las cámaras en espacios públicos, se recomienda usar mascarilla o vestimenta que tape el rostro, ya que la tecnología que usan las cámaras en Perú no cubre la identificación cuando las personas tienen las mascarillas puestas. Concientizar sobre esta necesidad puede ser vital para combatir el estigma alrededor del ejercicio del derecho a la protesta.

9. Acecho y 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).

---

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.

[7] 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

También 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[8]. Para que proceda la solicitud de acceso a los datos de geolocalización, debe tratarse de (i) flagrante delito o investigaciones preliminares por ciertos delitos[9], (ii) 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[10]. 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[11].

La obtención de datos personales es otro mecanismo basado en la **ingeniería social** que podrían utilizarse para averiguar dónde vive una persona o dónde se reúne para realizar activismo. Aunque una persona no se dé cuenta, mucha de su información online puede dar pistas a adversarios sobre los lugares que frecuenta o vive. Por ejemplo, fotos o menciones a lugares como restaurantes o cafeterías.

Recomendaciones

En materia de autocuidado, recomendamos que las personas eviten hacer publicaciones sobre los lugares que frecuentan o que sean fáciles de identificar por sus características. Otra recomendación es no hacerlas mientras se está en el lugar, sino en otro momento, para evitar el seguimiento. Aunque es menos probable, es recomendable retirar el etiquetado GPS a las fotos que se capturan con la cámara del celular.

Por otro lado, creemos que es importante, como sociedad civil, posicionarnos contra la posibilidad de geolocalización sin disposición fiscal ni orden fiscal que trajo el Decreto Legislativo 1182. En julio del 2021, el Congreso de la República aprobó la Ley 31284, que modifica el Decreto Legislativo 1182[12] y amplía la posibilidad de geolocalización, más allá de la flagrancia delictiva, para las investigaciones preliminares de ciertos delitos, cuestión que nos moviliza como sociedad civil. Asimismo, en caso se encuentre que es frecuente la práctica de seguimiento o vigilancia arbitraria de domicilios, se pueden tener modelos de hábeas corpus que empoderen a la ciudadanía para demandar estos hechos.

10. Uso de la fuerza

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[13].

---

[8] Reglamento de la Ley de la Policía Nacional del Perú, art. 128

[9] Están comprendidos aquí los delitos contra la vida, el cuerpo y la salud; contra la libertad, contra el patrimonio, contra la administración pública, de lavado de activos, de trata de personas, de tráfico ilícito de drogas, de minería ilegal y los comprendidos en la Ley 30077, Ley contra el Crimen Organizado.

[10] Decreto Legislativo 1182, arts. 3 y 4

[11] Ley que regula el Régimen Disciplinario de la Policía Nacional del Perú (Ley 30714), tabla de infracciones y sanciones.

[12] Enlace: https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1182-decreto-legisl-ley-n-31284-1973481-3/

[13] 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)

Recomendaciones

Es urgente una reforma policial para evitar agresiones como el uso indiscriminado y desproporcionado de la fuerza. En ese sentido, como sociedad civil tenemos un llamado a seguir articulando y convocando voceros para poner en la agenda pública la necesidad de contar con una PNP respetuosa de los derechos humanos. Asimismo, podemos orientar a la ciudadanía para que conozcan en detalle sobre las vías penal y administrativa mediante las cuales pueden denunciar las lesiones correspondientes. En el caso de la vía administrativa, consideramos muy importante que se genere un ambiente en el que todos estos casos sean denunciados ante la Inspectoría General, de modo que tengamos un diagnóstico aproximado de cuántas incidencias de este tipo ocurren.

GLOSARIO

- **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 imagen 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.