CHÉCHERES, JUGUETES Y ARMAS

Un inventario parcial de las **tecnologías** que utiliza la **Policía Nacional en Colombia**

20 años Fundación Karisma

CHÉCHERES, JUGUETES Y ARMAS

Un inventario parcial de las **tecnologías** que utiliza la **Policía Nacional** en Colombia

Investigación:

Línea de Partición Cívica
Laboratorio de Seguridad Digital y Privacidad (K+LAB)

CONTENIDO

INTRODUCCIÓN

La seguridad es quizá una de las áreas en que las soluciones tecnológicas se venden con más facilidad como efectivas, innovadoras y capaces de resolver problemas estructurales como la violencia, la criminalidad o, incluso, la corrupción. La Policía Nacional no ha sido ajena a esta tendencia y ha estado adquiriendo distintos tipos de tecnologías que, en teoría, aumentan sus capacidades de lucha contra la delincuencia. No obstante, no tenemos certeza sobre la efectividad de estas nuevas herramientas, del uso que les están dando, ni de sus capacidades. A ciencia cierta, lo único que sabemos es que tienen estas tecnologías en su poder y que muchas de ellas ponen en riesgo algunos derechos fundamentales de la ciudadanía.

Desde la Fundación Karisma, guiados por nuestro propósito de garantizar que el uso de nuevas tecnologías en el sector público no tenga consecuencias negativas para el ejercicio y garantía de los derechos humanos, realizamos un seguimiento cercano a las tecnologías adquiridas y usadas por la Policía.. Conocer los dispositivos, los softwares y las técnicas que utiliza la fuerza pública permite realizar una veeduría más eficiente con el fin de ejercer control y evitar abusos.

Este documento es un aporte inicial que plasma lo que sabemos y lo que no sobre las tecnologías que están a disposición de la Policía, así como los vacíos de información que hemos identificado. Este es un punto de partida que establece un mapeo general e indica una dirección que permita avanzar en términos de investigación e incidencia. El inventario enumera nueve tipos de tecnología especificando lo que sabemos, lo que nos preocupa y lo que proponemos al respecto de cada una.

Por último, este breve listado también busca desmitificar algunas ideas abstractas que solemos tener sobre lo que la Policía puede y no puede hacer utilizando tecnologías, pues creemos que precisamente muchos de los problemas en su implementación surgen de nuestro desconocimiento acerca de cuáles son las capacidades y los alcances reales de estos sistemas. Este es un pequeñísimo manual para distinguir la realidad de la ciencia ficción y así poder hacer frente a las máquinas sin temores infundados.

TIPOS DE TECNOLOGÍA

1 PROGRAMAS DE EXTRACCIÓN DE INFORMACIÓN FORENSE

¿Qué son?

Los programas forenses son herramientas que sirven para extraer información de equipos digitales como computadores, celulares, discos duros, cámaras o drones, entre otros. Aprovechan vulnerabilidades de los sistemas operativos y de programas específicos para evadir contraseñas u otras barreras impuestas por las personas usuarias para acceder a la información en los dispositivos. Estos programas "llevan a cabo una copia exacta de un medio de almacenamiento digital, el cual se realiza a bajo nivel, esto mediante la copia bit a bit de todos los datos"[1]. Su capacidad es amplia y permite desencriptar[2] y autentificar[3] archivos. Generalmente, son usados en investigaciones judiciales.

La información extraída puede incluir aspectos técnicos del dispositivo (el número de serie, su fecha de manufactura, el sistema operativo que utiliza) y contenidos almacenados (documentos,

1 Duriva. ¿Qué es una copia forense o imagen forense. S.F. Disponible en: https://duriva.com/que-es-una-copia-forense-o-imagen-forense/

2 Romper la seguridad impuesta por el usuario con contraseñas y cifrado para hacer legibles archivos que estaban protegidos.

3 Constatar que los archivos no han sido modificados.

imágenes, audios, conversaciones en aplicaciones de mensajería, información de cuentas e inicios de sesión, entre otros). A partir de la información extraída se pueden generar perfiles y establecer redes de contactos.

¿Qué nos preocupa?

El uso de software de extracción de información forense requiere que los equipos de los que se va a extraer la información sean conectados al dispositivo con el sistema de extracción. Es decir que la Policía necesita acceso físico al dispositivo cuya información quiera copiar Con esto en mente, las denuncias ciudadanas sobre requisas a celulares son alarmantes, pues que la Policía tenga en su poder un celular implica la posibilidad de que se copie la información..

Por otro lado, las capacidades de los softwares de extracción resultan desproporcionadas (aún en los casos de investigaciones judiciales) pues permiten acceso a la totalidad de la información almacenada en un equipo, sin distinción alguna y con la posibilidad de realizar una copia exacta. Dado el carácter íntimo de mucha de la información dentro de un dispositivo (fotos, chats, contactos en celulares o computadores) este tipo de tecnología usada sin control puede vulnerar derechos fundamentales como el de la intimidad, libertad de expresión, de participación, de protesta, de reunión, entre otros.

¿Qué proponemos?

- El acceso, uso, recolección y almacenamiento de la información extraída mediante software forense debe estar limitado únicamente a las dependencias de la policía con funciones judiciales y bajo la supervisión de un juez.
- La circulación y supresión de la información copiada, o parte de ella, debe evaluarse caso a caso por un juez de control de garantías.
- Establecer legalmente la obligación de notificar a la ciudadanía cuyos equipos hayan sido sometidos al uso de programas de extracción forense.
- Establecer la obligación legal de entregar una copia de la información extraída a personas cuyos equipos hayan sido sometidos al uso de programas de extracción forense.
- Establecer legalmente la obligación para la Policía de garantizar la integridad de los equipos y la información sometida al uso de programas de extracción forense.

El acceso a dispositivos mediante software forense solo se puede realizar en el marco de una investigación judicial, con orden del fiscal y control por parte del juez en 24 horas.

En relación con celulares, los agentes de policía únicamente pueden solicitar el IMEI. En este caso, no pueden manipular el celular si la persona dueña no lo permite; la persona puede marcar al *#06# y mostrar el número que aparece en pantalla.

En el contexto del Paro Nacional de 2021, hubo requisas y "decomisos" de equipos celulares no justificados. Con esta tecnología es posible que hubieran accedido a la información de los dispositivos.

2 IMSI CATCHER

¿Qué son?

Un IMSI catcher es un dispositivo que simula ser una torre de telefonía móvil y "engaña" a los celulares cercanos para que se conecten a él sin que las personas lo sepan. Esto permite capturar información relacionada con los teléfonos celulares y sus comunicaciones y, en muchos casos, calcular la ubicación del teléfono. Con los dispositivos más sofisticados se puede recopilar códigos IMSI (el identificador internacional del suscriptor móvil, por sus siglas en inglés, que es un número único asociado a cada tarjeta SIM) de un área en particular. IMSI también permite controlar, bloquear o degradar la señal, conocer el contenido de llamadas y mensajes de texto, e incluso, modificarlos.

Estos dispositivos no pueden interceptar contenidos encriptados como los mensajes de WhatsApp o Signal, pero pueden obtener los metadatos asociados a estas comunicaciones como la hora, la fecha, o la IP de los teléfonos.

¿Qué nos preocupa?

Este tipo de herramientas se consideran de vigilancia masiva porque al recoger datos de equipos en un área determinada no discriminan en contra de quién están dirigidas. Mediante el número IMSI y consultando la base de datos de registro de celulares pueden identificar a las personas titulares de las tarjetas e inferir quiénes estuvieron en un lugar y momento específico.

Además, a través de un IMSI catcher se puede recoger mucha más información de la que puede estar justificada por un fin legítimo como por ejemplo la información sobre el contenido de las comunicaciones e información sobre con quién se comunican las personas. Es decir, en algunos

casos estos dispositivos pueden utilizarse como tecnologías de interceptación.

Actualmente no hay regulación para este tipo de dispositivos en Colombia; no hay límites claros para sus usos permitidos, ni para su capacidad de vigilancia masiva, ni para su capacidad de tecnologías de interceptación.

En el marco de una protesta, el uso del IMSI Catcher podría permitir a la Policía conocer quiénes son las personas manifestantes, qué dicen en sus llamadas y dónde se encuentran, vulnerando la posibilidad de protestar anónimamente y aumentando los riesgos de persecución y perfilamiento. Además, en la medida en que puede utilizarse para bloquear la señal, también puede implicar riesgos para la seguridad de las personas que se están manifestando al impedirles comunicarse o transmitir videos e información sobre lo que ocurre durante la protesta.

Por ejemplo, en 2014 en Ucrania[4], MSI Catcher fueron usados para enviar mensajes intimidatorios a personas que se encontraban cerca de los lugares de protesta. De igual manera en Inglaterra[5] Se estableció que también fueron usados durante protestas pacíficas.

¿Qué proponemos?

- Es necesario que el Estado haga públicas las capacidades de los IMSI Catchers en su poder.
- Definir límites claros para los distintos usos permitidos y prohibidos de los IMSI catcher, así como los contextos en que pueden usarse y los mecanismos de control para garantizar que dichos límites se cumplan efectivamente (por ejemplo, exigiendo una autorización previa judicial).
- Es necesario crear una política que permita determinar de forma clara qué entidades del Estado y en ejercicio de qué funciones pueden usarse IMSI Catchers.
- Se debe Eestablecer legalmente la obligación de informar a la ciudadanía, por solicitud, si sus equipos han sido individualizados mediante IMSI Catchers y qué información se consiguió a partir de su uso.
- Debe reconocerse explícitamente que los datos recogidos por este medio están cobijados por la ley 1581 de 2012 sobre protección de datos personales.

4 Así se está usando el teléfono móvil como herramienta (y arma) en las protestas de Ucrania. 2014 Disponible en: https://www.xatakamovil.com/movil-y-sociedad/asi-se-esta-usando-el-telefono-movil-como-herramienta-y-arma-en-las-protestas-de-ucrania

5 VICE News Investigation Finds Signs of Secret Phone Surveillance Across London. 2016. Disponible en: https://www.vice.com/en/article/bjkdww/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london

Aunque los IMSI Catcher son tecnologías potentes, mucho de lo que esta tecnología puede hacer también puede realizarse mediante el acceso directo que tienen la Fiscalía a la infraestructura de los operadores telefónicos. En este sentido, imponer límites a los IMSI Catchers es importante, pero lo es más, garantizar la transparencia de los procedimientos de la policía judicial que involucran monitoreo o interceptación de comunicaciones.

Si quieres saber más sobre acceso directo, te recomendamos revisar el informe: Dónde están mis datos.

3 RECONOCIMIENTO FACIAL

¿Qué es?

El reconocimiento facial es una técnica, hoy en día automatizada y potenciada con inteligencia artificial, que permite contrastar la imagen de un rostro con imágenes almacenadas en una base de datos para tratar de identificar a la persona.

La Policía cuenta con el Sistema Automatizado de Identificación Biométrica (ABIS), conectado con la base de datos de identificación biométrica de la Registraduría Nacional del Estado Civil (RNEC) que tiene registro de huellas dactilares y de rostros. El ABIS le da capacidades a la Policía para identificar a personas a partir de vídeos e imágenes en las que se puedan ver los rostros. Las imágenes no tienen que haber sido captadas por las cámaras de la Policía, pueden provenir de cualquier fuente. Entre mejor sea la calidad y la iluminación, y más despejada y frontal esté la imagen del rostro, más probable será que el software logre identificar acertadamente a la persona. Por el contrario, si la imagen es de mala calidad, oscura, o si el rostro está ladeado o cubierto con tapabocas, gorras, gafas oscuras o bufandas, por ejemplo, es menos probable que el sistema encuentre coincidencias o que estas sean confiables.

En 2019, un día antes del inicio de las protestas del 21N, la Policía anunció en medios de comunicación que un helicóptero equipado con tecnología de reconocimiento facial sobrevolaría Bogotá para identificar a las personas que se manifestaran violentamente. Sin embargo, no hay evidencia de que alguien haya sido judicializado como resultado del uso de esta herramienta y, al parecer, se trató de una acción dirigida a disuadir a la ciudadanía de salir a protestar.

¿Qué nos preocupa?

El reconocimiento facial podría permitir identificar a las personas sin que ellas sepan que están siendo identificadas, es decir, sin su consentimiento, y de manera posterior a la captura de una imagen del rostro. Esto hace que el anonimato en la vía pública pueda llegar a ser efectivamente imposible, salvo que se oculte el rostro. En términos prácticos, el uso del ABIS implica tratar a todas las personas como sospechosas, haciendo caso omiso al principio de presunción de inocencia. Además, constituye una desproporción en los medios, pues se puede aplicar indiscriminadamente sobre toda la población.

Por otro lado, la sensación de estar siendo permanentemente vigilado produce un efecto inhibitorio (chilling effect) que puede desalentar el derecho a la reunión o a la protesta pacífica, entre otros, e incluso tener un efecto negativo sobre la salud mental. Hemos visto con preocupación que esta tecnología se despliega de manera discriminatoria, por ejemplo, en estadios de fútbol, presumiendo que los hinchas son una población que debe ser vigilada con más rigor.

Sumado a esto, en la medida en que esta tecnología –como todas– es imperfecta, hay casos de falsos positivos (identificación errada) y casos de falsos negativos (no identificación cuando sí debería ocurrir) que pueden conducir a falsas atribuciones o exoneraciones de responsabilidad. Esto es particularmente preocupante dado que la tecnología, por haber sido desarrollada con rostros de hombres blancos como referente, tiende a fallar más con rostros racializados, de mujeres y de personas mayores.[6] Como se mencionó antes, las condiciones lumínicas, la calidad de la imagen o el ocultamiento intencional del rostro, entre otras, también pueden hacer que los resultados sean menos confiables.

Por último, la tecnología de reconocimiento facial no cumple ningún fin preventivo, pues sólo puede usarse –en ciertos casos– para individualizar a responsables de conductas ilegales a posteriori, lo que alimenta una visión punitivista del quehacer policial y de la administración de justicia.

¿Qué proponemos?

- La base de datos de la RNEC no debería incluir registros biométricos faciales, pues su simple existencia facilita el uso abusivo de la tecnología de reconocimiento facial.
- De mantenerse la base de datos, es indispensable trazar límites claros a los usos posibles y a las instancias dentro de la Policía que tienen

6 Fundación Karisma. Qué es y cómo funciona el reconocimiento facial. 2021. Disponible en: https://digitalid.karisma.org.co/2021/07/01/que-es-reconocimiento-facial/.

acceso a esta información. Dichos límites deben excluir la vigilancia masiva y el perfilamiento. Deben existir estándares claros para definir su validez como herramienta de individualización e identificación, siempre mediada por autorización judicial.

- Debe haber transparencia sobre la capacidad técnica de la herramienta, así como auditorías que permitan determinar su confiabilidad o fiabilidad.
- Se debe garantizar la seguridad digital de los registros biométricos almacenados en la base de la RNEC para evitar usos ilegítimos o fugas de datos.
- Establecer legalmente la obligación para la Policía de informar a las personas cuando han sido identificadas usando biometría facial o dactilar. Siempre deben entregarse los datos del caso a la persona identificada (lugar, hora, fecha, motivo, la imagen contrastada junto con la explicación de su procedencia, etc.) y los detalles técnicos (tasa de confiabilidad del resultado, etc.).

Según la respuesta de la RNEC a nuestros derechos de petición, "solo hay dos entidades públicas autorizadas para realizar búsquedas en sus bases de datos biométricas: la Policía Nacional de Colombia y la Fiscalía General de la Nación, convenio 046 de 2017 y convenio 021 de 2018, respectivamente."[7] Sin embargo, no se especifica qué instancias dentro de la Policía Nacional pueden acceder a dichas bases.

También está la pregunta central sobre si, para acceder a estos datos, la Policía necesita una orden judicial. Normalmente tendría que ser así, pero esta tecnología parece estar en un terreno gris.

Más información sobre esta tecnología aquí:
El sistema multibiométrico ABIS de la Policía Nacional

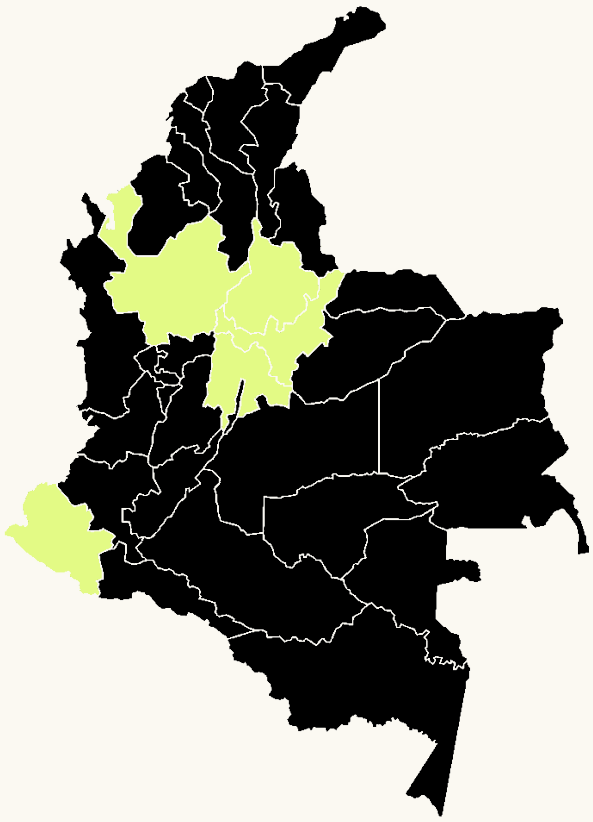
7 Registraduría Nacional del Estado Civil. Acceso a la base de datos biométrica. Disponible en: https://registraduria.gov.co/-Acceso-a-la-base-de-datos-biometrica-825-.html

4 CÁMARAS CORPORALES

¿Qué son?

LLas cámaras corporales, también llamadas cámaras unipersonales o *bodycam*s, son dispositivos de grabación de video y sonido que pueden fijarse a la ropa de un agente de policía, usualmente a la altura del pecho, los hombros o la cabeza; sirven para registrar el actuar de los agentes de policía en el marco del servicio. Usualmente imprimen al video la fecha, la hora, el número de serie correspondiente a la cámara e información sobre el modelo de la misma, estos elementos permiten ubicar las grabaciones temporalmente y asociarlas a un agente en particular. Estas grabaciones pueden ser usadas como materialprobatorio[8]. Algunos modelos pueden contar con capacidades adicionales como visión nocturna, reconocimiento facial en tiempo real, capacidad de conservar los dos minutos previos de vídeo anteriores a la activación voluntaria de la cámara o la capacidad de reproducir los videos grabados en una aplicación móvil, entre otras[9].

Mapa. Cobertura geográfica de cámaras unipersonales



Fuente Policía Nacional de Colombia 2021

8 Ver resolución 1091 de 2023. Procedimiento de actuación de la Unidad de Diálogo y Mantenimiento del Orden (UNDMO)

9 Axon. Products/Camera. Disponible en: https://www.axon.com/products/axon-body-2

Para 2021, la Policía Nacional tenía cámaras corporales en 5 departamentos. Actualmente no hay claridad acerca de la implementación de los pilotos de uso de cámaras corporales estipulados a partir del CONPES 4064 de 2021, puesto que en 2023 la adquisición de los dispositivos presentó irregularidades que ahora son investigadas por la Fiscalía[10]. A pesar de esto, a nivel distrital sí hay evidencia de compra e implementación de cámaras[11].

Según el Conpes 4064 de 2021, estos dispositivos registran y emiten el video y audio en tiempo real, hacia centros de monitoreo. Por ejemplo, en declaraciones públicas, la alcaldía de Bogotá ha dicho que el material registrado con las bodycams es transferido al sistema de videovigilancia de la ciudad.[12]

Los agentes de la Policía que acompañan las manifestaciones pueden portar cámaras corporales.

¿Qué nos preocupa?

No conocemos con exactitud los modelos ni las capacidades de las cámaras utilizadas en Colombia. Por ejemplo, desconocemos si son capaces de hacer reconocimiento facial en vivo o se pueden vincular con sistemas de reconocimiento facial en tiempo real o si sus grabaciones sólo quedan alojadas en servidores remotos o también en archivos locales de respaldo. No está claramente regulado quién custodia los servidores en donde se almacena la información, quién tiene acceso a los videos, si es necesario tener una orden judicial para ello, por cuánto tiempo se almacenan, ni quién puede borrarlos y en qué condiciones. Esto puede tener importantes implicaciones pues si la Policía puede tener acceso privilegiado es posible que manipulen o destruyan la información, ajusten sus declaraciones a lo que ocurre en un video antes de que la contraparte haya tenido la oportunidad de verlo, o que restrinjan el acceso de otros al contenido con la finalidad de dificultar denuncias o procesos de investigación.

Así mismo, nos preocupa que, dado el vacío regulatorio, no es claro si los agentes pueden encender y apagar las cámaras a voluntad, lo que implicaría que pueden detener (o comenzar) la grabación en momentos decisivos. También es problemático que puedan grabar a las y los ciudadanos sin su consentimiento e incluso sin su conocimiento.

Por último, y dado que las cámaras pueden transmitir información en tiempo real por medio de la red de datos móviles, es posible que las cámaras operen con muy diferentes niveles de fiabilidad en distintos espacios de acuerdo con las condiciones de conectividad, lo que significa una menor capacidad de veeduría en zonas remotas o artificialmente desprovistas de señal (ver aparte sobre jammers).

10 Revista Semana. Bodycams, un escándalo anunciado en la Policía por cuenta de un millonario y frustrado contrato de cámaras corporales; la Fiscalía investiga. 2023. Disponible en: https://www.semana.com/nacion/articulo/bodycams-un-escandalo-anunciado-en-la-policia-por-cuenta-de-un-millonario-y-frustrado-contrato-de-camaras-corporales-la-fiscalia-investiga/202300/

11 El Tiempo. Alcaldía entrega 400 cámaras unipersonales bodycam a la Policía. 2023. Disponible en: https://www.eltiempo.com/bogota/claudia-lopez-entrega-400-camaras-unipersonales-bodycam-a-la-policia-744506

12 íbidem

El uso de cámaras corporales no debería afectar los derechos de los y las manifestantes porque su finalidad es fiscalizar el actuar de la Policía. Su uso debe estar restringido a ese propósito y no a vigilar a la ciudadanía o las manifestaciones públicas[13].

Para que las cámaras corporales sean una herramienta eficiente de veeduría sobre el actuar policial es indispensable que el control narrativo no esté en manos de la misma institución, pues se pierde la objetividad de la herramienta. Es decir, el principio de publicidad de las actuaciones policiales debe estar garantizado, aquí también, mediante regulaciones claras que exijan grabaciones íntegras durante los procedimientos, acceso equitativo a todas las partes legítimamente interesadas y garantías de la integridad de la información.

¿Qué proponemos?

- Los agentes de policía que porten cámaras corporales deberán grabar toda su actividad cuando se encuentren en el ejercicio del poder y la función judicial.
- La Policía deberá garantizar la idoneidad técnica de las cámaras. Cada uno de los agentes que porten cámaras corporales tiene la tarea de asegurar la integridad del contenido grabado y estos podrán ser sancionados en los casos en que no existan grabaciones de su quehacer sin que medie justificación suficiente para ello. Habrá un protocolo para garantizar la transmisión y el almacenamiento de información en los servidores.
- Las imágenes siempre deberán ir acompañadas de los datos y metadatos relevantes para garantizar la no manipulación de la información (estampillas de fecha y hora, así como número de serie de la cámara asociado a su portador).
- Los agentes de Policía deben informar a las y los ciudadanos que su imagen está siendo registrada y deben cesar la grabación si la persona así lo solicita, salvo en los casos en que el agente tenga razones para sospechar que la persona ha cometido o está cometiendo un delito.
- Los servidores que alojan el material grabado deben tener mecanismos que le permitan a una entidad de control externa a la Policía Nacional

13 ACLU. A Tale of Two Body Camera Videos. 2020. Disponible en https://www.aclu.org/news/privacy-technology/a-tale-of-two-body-camera-videos

hacer veeduría de la integridad, disponibilidad y seguridad de los datos. Por sus funciones, esta entidad debe ser la Procuraduría General de la Nación.

- La información captada por las cámaras corporales debe estar disponible para todas las partes que tengan un interés legítimo por conocer su contenido, respetando siempre las garantías de privacidad, defensa y debido proceso de las personas cuyas imágenes fueron registradas.

5 DRONES

¿Qué son?

Son vehículos aéreos no tripulados controlados remotamente. Suelen venir equipados con cámaras y podrían estar habilitados con tecnología de reconocimiento facial, altavoces, radares y herramientas de interceptación de comunicaciones –como los IMSI catchers– o de bloqueo de señales –como jammers–.

Los drones con cámara pueden utilizarse para vigilar y seguir a distancia los movimientos de los y las manifestantes. Cuando están equipados con tecnologías para interceptar comunicaciones, pueden utilizarse para vigilar, rastrear e intervenir sus llamadas y mensajes de texto (ver aparte de IMSI catchers) y, de igual forma, cuando están equipados con aparatos de bloqueo de señal pueden impedir la entrada y salida de comunicaciones (ver aparte de jammers). Los drones equipados con altavoces pueden usarse para dar órdenes, instrucciones o advertencias a quienes protestan. Por lo pronto, no tenemos noticia de que existan drones equipados con armamento en Colombia.

En 2019, la policía en colombia adquirió drones, pero no tenemos certeza de sus características técnicas, sus capacidades y sus usos en el contexto de la protesta. Si los drones únicamente incorporan cámaras de vídeo, la única diferencia con las cámaras de vigilancia instaladas en las ciudades o las cámaras corporales, es la capacidad de seguir físicamente a sus objetivos sin la presencia física de agentes de policía. Si incorporan otras tecnologías como reconocimiento facial, IMSI catchers, jammers o armamento, suponen un riesgo a la privacidad, a la posibilidad de manifestarse anónimamente e incluso a la integridad física de la ciudadanía.

¿Qué nos preocupa?

Con respecto a la capacidad de grabación de video y audio de los drones, las preocupaciones son las mismas que con las cámaras corporales y aplican las mismas consideraciones mencionadas arriba, entre otras: no es claro cómo se almacena la información captada por las cámaras de los drones ni quién custodia los servidores. Además de lo anterior, los drones pueden volar a alturas en que es prácticamente imposible notar su presencia, lo que permite grabar a las personas sin que ellas lo sepan.

Sin embargo, como los drones pueden estar equipados con otras tecnologías, nos preocupa que se utilicen sin que sea claro para la ciudadanía cuáles son sus alcances. Esto hace que la veeduría y el control sobre su uso sea mucho más difícil y especulativo.

Finalmente, las denuncias de drones vigilando activistas, políticos o manifestaciones coinciden en que estos vehículos controlados a distancia no están identificados y no es posible saber si pertenecen al Estado o a particulares.

¿Qué proponemos?

- Es necesario regular qué capacidades tienen los drones de la Policía y en qué contextos se pueden usar. Por ejemplo, en contextos de manifestaciones públicas, su uso pone en riesgo derechos fundamentales y no debe ser permitido.
- Así mismo, los drones, tal como cualquier otro miembro y vehículo de la Policía, deben ser claramente identificables. Es decir, que deben portar luces específicas asociadas a la Policía y estar pintados con un color o insignia visible. Deben estar dotados de un número que haga posible su fácil identificación a distancia por parte de la ciudadanía. Esto permitiría además que las personas hagan efectivo sus derechos asociados con la Ley 1581 de 2012 sobre protección de datos.
- En ningún caso los drones deben estar equipados con armamento: ni con armas letales, ni con armas de menor letalidad, ni de letalidad reducida, ni de disuasión.

Precedentes de uso de drones en protestas en Colombia: *Marchas de este miércoles estarán vigiladas por drones y aeronaves*

6 OSINT

¿Qué es?

La inteligencia de Fuentes Abiertas (OSINT por sus siglas en inglés[14] cconsiste en una serie de técnicas para recolectar y analizar datos que se encuentren alojados en fuentes de información de libre acceso con fines ofensivos o defensivos (planeación de operaciones). Este tipo de tecnología es la parte técnica de las actividades de vigilancia que la Policía jurídicamente ha llamado "ciberpatrullaje". También se usa para actividades de inteligencia, investigación y vigilancia a la ciudadanía por parte de entidades como el Ejército, la Fiscalía y la DNI.

Los software OSINT tiene capacidades para realizar vigilancia masiva, ya sea monitorear tendencias enteras en redes sociales para clasificar el contenido y perfilar a personas usuarias de estas, o a través de técnicas de *web scrapping*[15] para descargar de forma masiva información disponible en buscadores de internet.

Finalmente, este tipo de sistemas permiten perfilamientos a partir de los cruces y análisis de información disponible en internet, lo que incluye: contactos, interacciones, ubicaciones señaladas, imágenes, entre otras. Algunos de los sistemas adquiridos por entidades estatales permiten realizar geolocalizaciones y desanonimización de perfiles.

¿Qué nos preocupa?

El uso de sistemas OSINT de forma abusiva afecta distintos derechos humanos. Para empezar, la vigilancia masiva y el etiquetado de contenido publicado por la ciudadanía afecta la libertad de expresión, pues disuade a la ciudadanía de opinar y publicar en redes sociales para evitar el accionar del Estado. Así lo señaló la Comisión Interamericana de Derechos Humanos (CIDH) en su informe de Observaciones y Recomendaciones a Colombia tras su visita durante el Paro Nacional de 2021[16].

14 Karisma. Cuando el Estado vigila. OSINT y Ciberpatrullaje en Colombia. Disponible en: https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/

15 Por web scrapping nos referimos al proceso automatizado de extracción de contenidos y datos de sitios web mediante software para su análisis posterior.

16 CIDH. Recomendaciones y observaciones: visita de trabajo a Colombia. Disponible en: https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

En segundo lugar, el uso de OSINT implica la adquisición de herramientas para acciones que el Estado sólo puede usar en procesos judiciales: acopio de material probatorio, individualizaciones, geolocalización de ciudadanos, pero también de otras que no puede utilizar: perfilamientos, borrado de búsquedas, copia masiva de información. Por tanto, resulta urgente regular la materia de forma garantista para la ciudadanía.

Finalmente, no existe mucha información pública sobre cómo se está usando la tecnología OSINT del Estado y lo que se conoce implica vulneraciones a derechos humanos: ya sea con perfilamientos a periodistas[17], etiquetado de publicaciones ciudadanas[18] o para acopiar pruebas que sirvan para imponer medidas de aseguramiento. Sumado a ello, la información sobre la tecnología en sí no es abundante, por lo tanto, es difícil hacer control ciudadano sobre las características de las herramientas como sobre su uso[19].

¿Qué proponemos?

- Es necesario que se regule de forma clara en ejercicio de qué funciones legales la Policía podrá utilizar software OSINT. En ningún caso se debe usar para realizar actividades ilegales como vigilancia o monitoreo masivo y debe existir un marco sancionatorio ejecutivo para los casos de excesos.
- El uso de OSINT para la recolección de material probatorio debe ser objeto de reglamentación legal para garantizar los derechos a la defensa y el debido proceso de los investigados.
- Es fundamental establecer controles internos sobre el uso de sistemas OSINT, entre los cuáles deben disponerse contrapesos institucionales y medidas de transparencia como registro de los actores que acceden a la información recopilada, informes periódicos a los órganos de control e informes públicos de rendición de cuentas.
- La adquisición de sistemas OSINT justificada en objetivos de seguridad nacional, debe ser restrictiva y con estricto cumplimiento de los requerimientos legales para que ese tipo de contratación proceda. En

17 El Tiempo. Los "trabajos especiales" de inteligencia por los que irán a juicio disciplinario 13 militares. 2020. Disponible en: https://www.elespectador.com/judicial/los-trabajos-especiales-de-inteligencia-por-los-que-iran-a-juicio-disciplinario-13-militares-article/

18 Índice de Derechos Digitales. Ciberpatrullaje de la Policía Nacional para identificar desinformación. 2023. Disponible en: https://indicederechos.digital/docs/CiberpatrullajeDesinformacion/

19 La punta del Iceberg. Transparencia del OSINT en Colombia. Disponible en: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia/

ningún caso las dependencias de la Policía deben adquirir herramientas de vigilancia masiva aludiendo a la seguridad nacional cuando tenga objetivos de marketing organizacional o defensa de "derechos reputacionales".

- Los sistemas OSINT no deben ser usados para recopilar información que posteriormente sea categorizada como falsa o verdadera por parte de la Policía, o para realizar cualquier otra actividad para la que no sea competente.

Para más información sobre OSINT y ciberpatrullaje en Colombia

- ***Cuando el Estado Vigila: OSINT y ciberpatrullaje en Colombia***
- ***Inteligencia estatal tiene capacidades de vigilancia masiva y sin control: FLIP***
- ***La punta del iceberg. Los problemas de transparencia del OSINT en Colombia***

7 SIGINT

¿Qué es?

La inteligencia de señales (SIGINT por su abreviación en inglés[20]) es un conjunto de técnicas que sirven, generalmente, para interceptar señales distintivas emitidas por equipos electrónicos. En contextos policivos es usada generalmente para interceptar comunicaciones telefónicas o encontrar la localización de un celular o computador.

Con la inteligencia de señales es posible acceder al contenido de comunicaciones no cifradas aunque normalmente se vale del uso de criptoanálisis para tratar de descifrar comunicaciones o señales encriptadas. En Colombia, por ejemplo, los mensajes de texto y las llamadas telefónicas

20 ODIN. Osint e Inteligencia. Qué es SIGINT, Cómo se usa y ejemplos de la inteligencia de señales. Disponible en: https://odint.net/sigint/

no tienen cifrado, de modo que es posible acceder a su contenido. Existen herramientas que pueden ser catalogadas como de SIGINT que podrían ser usadas para bloquear señales (dejar a un equipo sin acceso a la red telefónica o internet) o determinar de forma muy precisa la ubicación de un dispositivo o qué dispositivos se encuentran en un lugar.

¿Qué nos preocupa?

Haciendo uso de SIGINT puede realizarse vigilancia de comunicaciones (monitoreo del espectro o interceptación de comunicaciones individualizadas) sin los controles propios de la actividad en el marco de una investigación judicial. Además, algunas herramientas catalogadas como de SIGINT permiten geolocalizaciones precisas y bloqueo de comunicaciones; este tipo de capacidades vulneran los derechos a la intimidad y la libertad de expresión.

¿Qué proponemos?

- Es necesario que el Estado haga públicas las capacidades y los alcances de los dispositivos de SIGINT en su poder.
- Es necesario definir límites claros para los distintos usos permitidos y prohibidos de los equipos de SIGINT, así como los contextos en que pueden usarse y los mecanismos de control para garantizar que dichos límites se cumplan efectivamente. Dado el alcance de este tipo de tecnología, estos dispositivos deberían ser usados únicamente en contexto de investigaciones judiciales y bajo la supervisión de un juez.
- Se debe establecer legalmente la obligación de informar a la ciudadanía, por solicitud, si sus equipos han sido individualizados mediante SIGINT y qué información se consiguió.
- Debe reconocerse explícitamente que los datos recogidos por este medio están cobijados por la Ley 1581 de 2012 sobre protección de datos personales.

8 JAMMERS

¿Qué son?

Un *jammer* o inhibidor de señal es un aparato electrónico que impide la comunicación de dispositivos tecnológicos a través de la obstrucción de las señales de los equipos que tiene a su alrededor. Esto se realiza a través de la transmisión de señales en la misma frecuencia que utilizan las redes móviles de celulares, equipos de posicionamiento global (GPS), WiFi o bluetooth, entre otras.

Un inhibidor es capaz de llenar de ruido o interferencias una frecuencia de transmisión impidiendo así que la información útil sea recibida, haciendo que el aparato receptor sea incapaz de diferenciar entre las múltiples señales trampa y la real. Es como si, para evitar que dos personas en un mismo lugar se puedan comunicar, un tercero pone música a todo volumen.

¿Qué nos preocupa?

Una característica de los *jammers* es la dificultad para ser detectados. Quiénes se ven afectados por ellos solo perciben problemas para establecer la comunicación. Es decir, las personas cuyas comunicaciones son bloqueadas mediante jammers no pueden saber que son víctimas de esta tecnología ni distinguirla de otras causas por las que pueden fallar las comunicaciones como la saturación o los problemas de infraestructura. Esto es preocupante porque su utilización puede realizarse sin controles, sin generar rastros y evitando controles judiciales.

Las interrupciones de señales causan dificultades de comunicación entre las personas y afecta directamente otros derechos como la libertad de expresión, de participación política o el de reunión al impedir el acceso a internet y otros medios de comunicación.

Finalmente, su utilización es desproporcionada dado que los *jammers* afectan a un número indeterminado de personas y contenidos.

¿Qué proponemos?

- Se debe regular la adquisición y uso de jammers, fijos y móviles, conforme a estándares de derechos humanos. Esto debe incluir la prohibición de usarlo en contextos como la protesta y establecer controles para su uso (registros, permisos e informes públicos).
- Se debe establecer la obligación de informar públicamente sobre el uso de jammers tanto por el Estado como por los operadores de internet cuándo los identifiquen.

- Se debe realizar un inventario de inhibidores en poder del Estado y sobre los usos legalmente necesarios y proporcionales de los mismos.
- En los casos que se utilicen jammers debe quedar constancia de la orden de usarlos, la cadena de custodia de los mismos y del lugar, fecha, hora, circunstancia y motivación por la que se utilizaron.

Sobre las sospechas de uso de jammers en protesta en Colombia: ***El misterio detrás de los cortes de Internet en Cali durante el paro de 2021.***

9 SISTEMAS DE PREDICCIÓN DEL DELITO

¿Qué son?

Los sistemas de predicción del delito son tecnologías de procesamiento y análisis de datos (por ejemplo, tasas de arresto, geolocalización de denuncias o bases de datos de criminales) que pretenden anticiparse a la comisión de delitos y sirven como base para tomar decisiones de políticas de seguridad (por ejemplo, la cantidad de patrullas asignadas a una zona, programas de monitoreo, distribución de cámaras de seguridad, dictar medidas de aseguramiento, etc.).

En Colombia tenemos registro de al menos dos sistemas de estas características utilizados por la Fiscalía General de la Nación (Watson Machine Learning y Prisma) y al menos uno operado por la secretaría de seguridad de Bogotá (Sistema predictivo de seguridad)[21]. Los adscritos directamente a la Policía Nacional son los descritos en el apartado sobre OSINT y al menos un contrato, adjudicado en 2021 a la unión temporal UT ETCO 2021 (conformada por ETraining SAS y Comware), que tenía por objeto el "desarrollo del modelo predictivo del delito para el centro de análisis criminal de la dirección de investigación criminal e Interpol", con presupuesto de 3.520 millones de pesos.

¿Qué nos preocupa?

Estos sistemas pueden ser muy diversos en sus capacidades y alcance, dependiendo de qué entidad los utilice, qué bases de datos los alimenten y, sobre todo, cuál sea su finalidad.

21 Gutiérrez, J. D., Muñoz-Cadena, S., Castellanos-Sánchez, M.Sistemas de decisión automatizada en el sector público colombiano. 2023. Universidad del Rosario. Disponible en: https://doi.org/10.34848/YN1CRT/8OHRT0

Sin embargo, algunas preocupaciones transversales tienen que ver con el hecho de que las bases de datos suelen tener sesgos de entrada, lo que puede redundar en comportamientos discriminatorios por parte de la fuerza pública, en la medida en que criminalizan más a poblaciones que históricamente han sido desproporcionadamente vigiladas y perseguidas. Es decir, refuerzan estereotipos y sesgos sobre criminalidad[22] con base en mediciones que, equivocadamente, se toman por objetivas e imparciales.

Uno de los principales aspectos problemáticos de estas tecnologías es su tendencia a desplazar la responsabilidad en la toma de decisiones que afectan derechos fundamentales de las personas. Esto, sobre la idea errónea de que las conclusiones derivadas de sistemas de inteligencia artificial son infalibles y justas, pues fueron hechas por máquinas.[23]

Por otra parte, hacer un control efectivo sobre estas herramientas es una tarea particularmente compleja en la medida en que, como en el caso de las herramientas de OSINT, su compra, desarrollo y utilización suele estar protegida por la reserva de seguridad nacional. De igual manera, las bases de datos utilizadas para su entrenamiento pueden tener sesgos ocultos difíciles de identificar[24] si únicamente se tiene acceso a los resultados y no se conocen los principios que operan el sistema.

En Colombia este tipo de herramientas se utilizan más para la administración de justicia que para la predicción del delito.[25] Sin embargo, la información disponible es limitada y merece más investigación.

¿Qué proponemos?

- Como regla general es deseable que no se utilicen estas tecnologías en ninguna decisión que pueda afectar derechos fundamentales. En el caso específico de la Policía los derechos afectados pueden ser la presunción de inocencia, el debido proceso, el juicio justo y el derecho a no ser discriminado, entre otros.

22 Dressel, J., Hany, F. The accuracy, fairness, and limits of predicting recidivism. 2018. DOI:10.1126/sciadv.aao5580

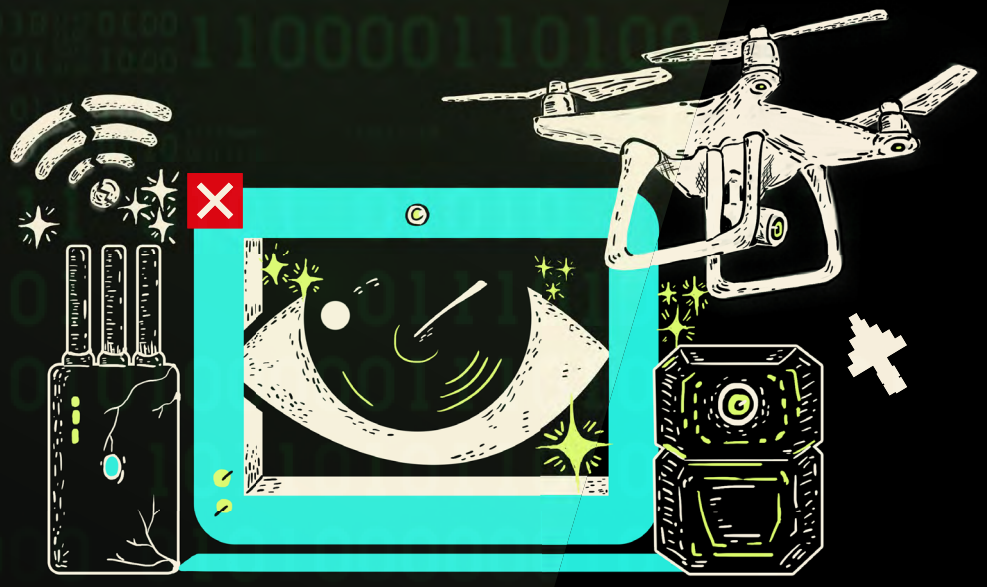
23 Egbert, S. About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany. 2018. https://doi.org/10.1007/s41125-017-0027-3

24 MIT Techonology Review. Predictive policing is still racist—whatever data it uses. 2021. Disponible en: https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/

25 Vea en SECOP II proceso número PN DIJIN SA MC 013 de 2021 entre la DIJIN y la Unión temporal UT Etco 2021.

- Hacer estudios de impacto sobre derechos humanos previos a su implementación y garantizar que las recomendaciones sobre los mismos sean vinculantes.
- Garantizar transparencia efectiva en el uso de estas tecnologías siempre que sean implementadas por el sector público.
- Garantizar el principio de “human-in-the-loop” o de supervisión humana para las decisiones algorítmicas, de manera que siempre las decisiones tomadas por este tipo de sistemas hayan sido revisadas por personas antes de hacerse efectivas.

20 años



fundacionkarismaa

karismacol

@Karisma

karisma.org.co