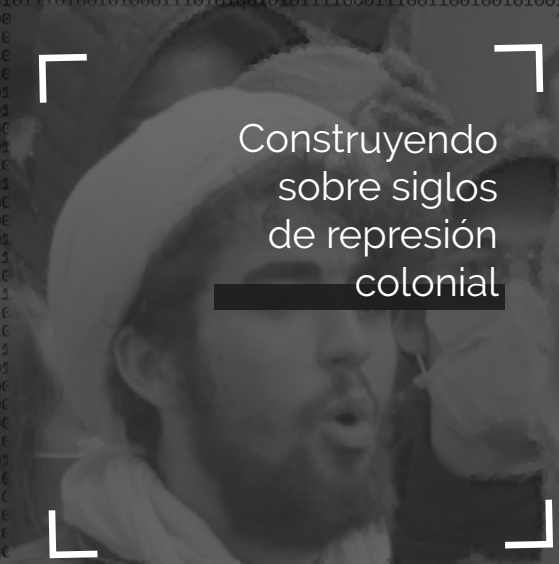
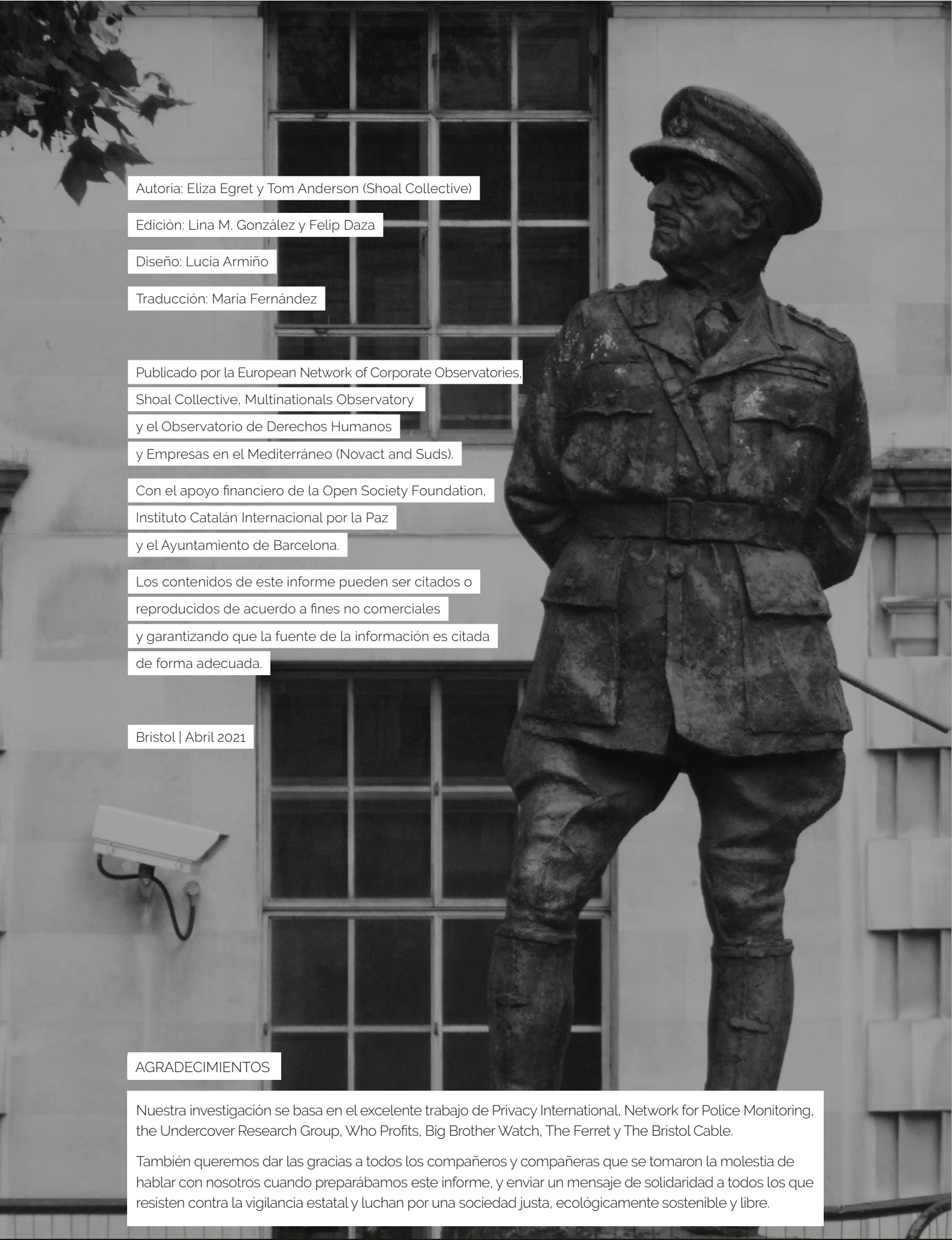
VIGILANCIA MASIVA Y CONTROL
DE LA DISIDENCIA EUROPEA

REINO UNIDO

Vigilancia de Estado: El caso de Reino Unido



ENCO
EUROPEAN NETWORK OF CORPORATE OBSERVATORIES
Observatoire des multinationales
SOCIAL, ÉCOLOGIQUE, POLITIQUE
ODHE Observatori de Drets Humans i Empreses a la Mediterrània
shoal radical writing for a world beyond capitalism



Autoría: Eliza Egret y Tom Anderson (Shoal Collective)

Edición: Lina M. González y Felip Daza

Diseño: Lucía Armiño

Traducción: María Fernández

Publicado por la European Network of Corporate Observatories,
Shoal Collective, Multinationals Observatory
y el Observatorio de Derechos Humanos
y Empresas en el Mediterráneo (Novact and Suds).

Con el apoyo financiero de la Open Society Foundation,
Instituto Catalán Internacional por la Paz
y el Ayuntamiento de Barcelona.

Bristol | Abril 2021

AGRADECIMIENTOS

Nuestra investigación se basa en el excelente trabajo de Privacy International, Network for Police Monitoring, the Undercover Research Group, Who Profits, Big Brother Watch, The Ferret y The Bristol Cable.

También queremos dar las gracias a todos los compañeros y compañeras que se tomaron la molestia de hablar con nosotros cuando preparábamos este informe, y enviar un mensaje de solidaridad a todos los que resisten contra la vigilancia estatal y luchan por una sociedad justa, ecológicamente sostenible y libre.

Este informe y el webdoc relacionado se enmarca en proyectos de investigación, sensibilización y educación coordinados por las organizaciones Suds y Novact y la colaboración de Shoal Collective y Observatoire des Multinationales. Los financiadores no son responsables de la información que contiene o del uso que se haga.

CONTENIDOS

METODOLOGÍA

Durante el proceso de investigación se han utilizado los siguientes métodos:

- Revisión de los sitios web de las empresas, la prensa del sector y la policía; así como de la información facilitada por los periodistas, investigadores y grupos de campaña.
- Solicitudes de Libertad de Información (FOI de Freedom of Information) a las fuerzas policiales y a los ayuntamientos, y utilización de información pública FOI a través del sitio web WhatDoTheyKnow.
- Búsqueda en el Diario Electrónico de Licitaciones de la UE.
- Búsqueda de contratos adjudicados por la policía y los organismos gubernamentales a través del Buscador de Contratos de Gov.UK y la Base de Datos de Adquisiciones Bluelight.
- Entrevistas con militantes, activistas y otros miembros del público afectados por la tecnología.
- Búsquedas en la base de datos de información empresarial Orbis de Bureau Van Dyck.

INTRODUCCIÓN

El Reino Unido tiene fama de ser un Estado vigilado, y con razón. En Londres hay una cámara de videovigilancia por cada 14 habitantes[1]. Las nuevas tecnologías de vigilancia, como el reconocimiento facial y los drones de la policía, son ya una realidad en todo el Reino Unido, y la legislación británica permite más vigilancia estatal de las comunicaciones privadas que cualquier otro país de Europa[2].

El Reino Unido es también uno de los mayores exportadores de tecnología de vigilancia, con empresas británicas que venden en el extranjero tecnología de pirateo telefónico, programas espía y software de reconocimiento facial[3].

Sin embargo, la vigilancia no es nada nuevo para el Estado británico. Tiene un largo historial de espionaje y vigilancia, que se ha perfeccionado en su subyugación de las poblaciones colonizadas en todo el mundo durante siglos. Sin embargo, la proliferación de las tecnologías digitales ha creado un entorno en el que el estado de vigilancia británico se ha intensificado hasta alcanzar niveles nuevos y profundamente invasivos, amenazando nuestra privacidad y nuestra libertad.

Este informe presenta una visión general del uso de diferentes tipos de tecnología de vigilancia en el Reino Unido, así como de las empresas que suministran los equipos. También examinamos cómo esta tecnología opresiva se está movilizando contra los movimientos sociales en el Reino Unido y cómo los efectos de la vigilancia se están dejando sentir de forma desproporcionada entre la clase trabajadora y las comunidades de color.

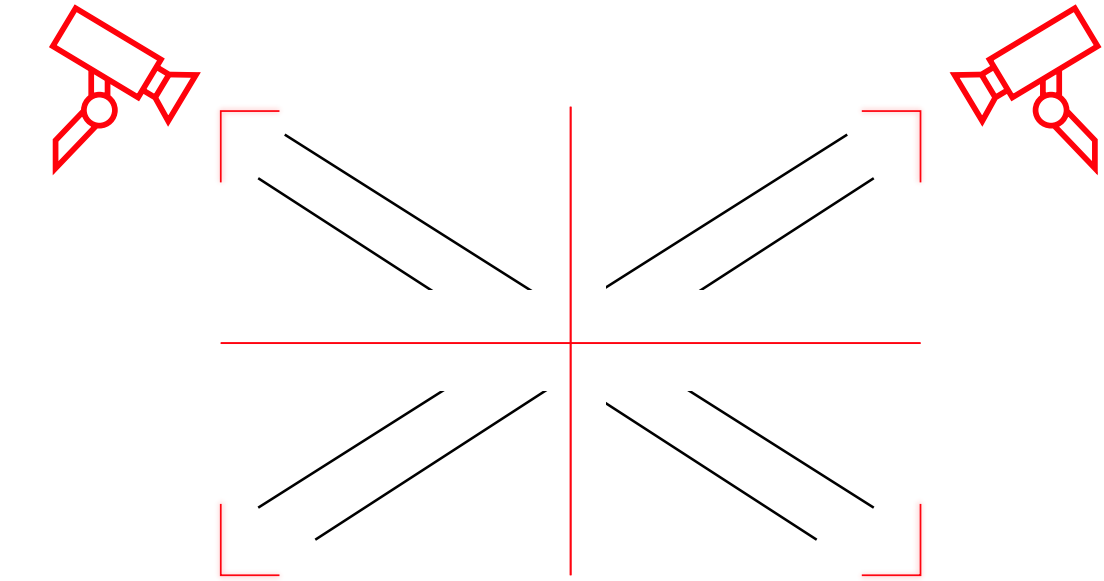
1 Keegan, M. August 14 2020, 'The most surveilled cities in the world', ***US News*** https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world [Accessed March 16, 2021].

2 Griffin, A. November 2016, 'Britain just got perhaps the most intrusive spying powers ever seen' ***The Independent***. https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html [Accessed March 12, 2021].

3 Privacy International, July 2016, 'The Global Surveillance Industry' https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf [Accessed March 16, 2021].

Vigilancia de Estado: El caso de Reino Unido

1 LA VIGILANCIA Y EL ESTADO BRITÁNICO



Reino Unido se está convirtiendo en una sociedad de vigilancia cada vez más tecnificada. Pero el uso de la vigilancia por parte del Estado británico no es nada nuevo. Como potencia colonial, el Imperio Británico recurrió en gran medida a la vigilancia estatal durante muchos siglos para someter a su control y pacificar a los pueblos ocupados. Lo que ha cambiado en los últimos años es el abanico de tecnologías represivas que están desarrollando y desplegando las empresas privadas, así como el aumento de la dependencia de la tecnología digital, lo que abre paso a una nueva era de vigilancia estatal masiva.

Del mismo modo, en las dos últimas décadas el gobierno británico ha aplicado políticas antiterroristas y ha evocado una narrativa de seguridad nacional que justifica el despliegue de tecnologías de vigilancia masiva con el pretexto de que permitirán mantener segura a la población. Los avances tecnológicos, unidos a esta narrativa de seguridad nacional, han permitido al Estado escalar su control social hasta niveles nunca vistos.

VIGILANCIA Y COLONIALISMO

La recopilación de datos sobre las poblaciones colonizadas ha permitido al Estado británico vigilar, controlar, manipular y dividir a las comunidades, un componente central de la estrategia británica de "divide y vencerás". Los datos recogidos han servido de base para las tácticas represivas desplegadas por el Estado británico contra las poblaciones colonizadas, en beneficio del Imperio Británico. Está fuera del alcance de este informe ahondar en el oscuro pasado colonial británico. Sin embargo, en el informe se encontrarán algunos ejemplos reveladores que relacionan el colonialismo con la vigilancia.

Irlanda, la colonia más antigua de Gran Bretaña, ha servido de campo de pruebas para el desarrollo y el perfeccionamiento durante siglos de las tácticas de vigilancia y control británicas antes de ser aplicadas en otros lugares. Tras la rebelión irlandesa de 1798, el Estado británico emprendió una vigilancia masiva de la población irlandesa, incluida la recopilación de estadísticas y datos del censo[4]. Los espías e informantes que se infiltraron en el movimiento republicano irlandés de la época desempeñaron un papel importante a la hora de comprometer la rebelión de 1798 y los posteriores intentos de derrocar el dominio británico[5]. Esta vigilancia permitió a los británicos controlar mejor a la población irlandesa y enfrentar a las poblaciones nacionalistas y unionistas[6].

4 McQuade, B. Neocleous, M. 2020, 'Beware: Medical Police', ***Radical Philosophy,*** https://www.radicalphilosophy.com/article/beware-medical-police. [Accessed March 12 2021].

5 *Óg Ó Ruairc, P. 2017,* 'Spies and informers beware!' ***History Ireland,*** https://www.historyireland.com/volume-25/issue-3-mayjune-2017/spies-informers-beware/ [Accessed March 12 2021].

6 Hadden, P. 1980, 'Divide and Rule (Introduction)', Marxists.org, https://www.marxists.org/history/etol/writers/hadden/1980/divrule/introduction.html [Accessed March 12 2021].

Los colonialistas británicos de la India de los siglos XVIII y XIX recopilaron sistemáticamente datos sobre la población sometida con fines fiscales y de control social. Tras la rebelión india de 1858 contra la Compañía Británica de las Indias Orientales, se intensificaron los esfuerzos para desarrollar un nuevo sistema de clasificación "científica" de la población con el fin de hacer posible la famosa estrategia británica de "divide y vencerás", que consolidó el dominio británico mediante la utilización de las divisiones entre las diferentes comunidades religiosas y castas de la India[7].

De hecho, se puede ver claramente que las tecnologías de la sociedad de vigilancia actual tienen raíces coloniales. Según Elia Zureik:

> ***"Es significativo que las herramientas básicas de vigilancia, tal y como las conocemos hoy en día (toma de huellas dactilares, elaboración de censos, elaboración de mapas y elaboración de perfiles, incluidos los precursores de la biometría actual) se perfeccionaron y aplicaron en entornos coloniales, especialmente por parte de los holandeses en el sudeste asiático, los franceses en África y los británicos en la India y en América del Norte"[8].***

Los gobernantes del mandato británico en Palestina se basaron en los métodos de vigilancia desplegados en la India. En los años posteriores a la Primera Guerra Mundial, los británicos introdujeron tarjetas de identificación como parte de su represión a la revuelta árabe de la década de 1930, junto con sistemas de control como vallas de seguridad, torres de vigilancia, sistemas de permisos y puestos de control fronterizo[9].

El uso de la vigilancia por parte del Reino Unido como estrategia colonialista se ha vuelto cada vez más tecnológica en las últimas décadas, reflejando los avances de la tecnología de vigilancia en general. Desde 2007, el Reino Unido ha utilizado aviones no tripulados o drones en Afganistán. Del mismo modo, las tropas británicas también han utilizado drones en Irak y Siria. El uso de estas aeronaves de alta tecnología permite mantener bajo vigilancia constante a poblaciones enteras repartidas por vastas zonas geográficas, en una medida que antes hubiera sido imposible. Además, se pueden realizar ataques aéreos mortales por control remoto y a distancia sin necesidad de desplegar tropas terrestres de ocupación[10]. El uso de la alta tecnología de vigilancia por parte de Gran Bretaña como herramienta en la guerra moderna es muy preocupante, pero un debate más profundo sobre la cuestión queda fuera del alcance de este documento.

7 Zureik, E. November 2013, 'Colonial Oversight', https://www.redpepper.org.uk/colonial-oversight/ [Accessed March 12 2021] and Tharoor, S. 2017, 'The Partition: The British game of 'divide and rule'', ***Al Jazeera,*** https://www.aljazeera.com/opinions/2017/8/10/the-partition-the-british-game-of-divide-and-rule/ [Accessed March 12 2021].

8 ***Ibid.***

9 ***Ibid.***

10 House of Commons Briefing Paper, October 2015, https://researchbriefings.files.parliament.uk/documents/SN06493/SN06493.pdf [Accessed March 12 2021].

CONSTRUIR UNA SOCIEDAD DE VIGILANCIA EN CASA

La vigilancia y el control empleados por el Estado colonialista británico en el extranjero también han servido de base para el desarrollo de un Estado de vigilancia nacional. Cuando las poblaciones se han rebelado, o han amenazado con sacudir o derribar el status quo, una de las respuestas del Estado ha sido vigilarlas, con el fin de adelantarse y pacificar cualquier resistencia. En ningún lugar se ha visto esto tan claramente como en el caso británico y la manera en que este ha lidiado con el norte de Irlanda, que todavía se encuentra bajo su dominio.

Desde 1969, el norte de Irlanda ha sido testigo del despliegue de una serie de tácticas de vigilancia por parte del Estado británico, especialmente contra su población nacionalista. Estas tácticas formaban parte de una estrategia de contrainsurgencia, que se basaba en unidades secretas encubiertas, en la detección de masas y en la vigilancia. Estas medidas acompañaban a tácticas colonialistas más agresivas y probadas, como el internamiento (encarcelamiento sin juicio), el despliegue militar en zonas urbanas, los puestos de control militares, los estados de excepción continuos, los asesinatos, las masacres, la tortura, la connivencia entre las fuerzas de seguridad del Estado británico y los grupos paramilitares leales, así como la infiltración de grupos republicanos[11]. Las comunidades fueron puestas bajo asedio, controladas y vigiladas durante décadas. Según Privacy International, el militarismo británico en el norte de Irlanda fue un factor clave que impulsó a las empresas británicas a fabricar cada vez más equipos de vigilancia[12].

11 The Pat Finucane Centre, 2017, 'Legacy of Colonialism', https://www.patfinucanecentre.org/legacy-colonialism [Accessed March 12 2021].

12 Privacy International, July 2016, 'The Global Surveillance Industry'. Page 31.

ESPIONAJE POLICIAL

A finales de la década de 1960, cuando la revolución y la rebelión estallaron en todo el mundo, se creó en Gran Bretaña una unidad policial encubierta especializada con el mandato de espiar a los grupos de la izquierda[13]. A lo largo de la década de 1970, los agentes encubiertos de la Special Demonstration Squad (SDS) se infiltraron en los movimientos antirracistas, de liberación negra, de solidaridad irlandesa, obreros, marxistas y anarquistas[14].

En los años 70 y 80, los Servicios de Inteligencia británicos crearon un Comité de Subversión en la Vida Pública para espiar a quienes participaban en la agitación industrial[15].

Los años 80 fueron un periodo de intensa lucha de comunidades racializadas de Gran Bretaña contra el racismo institucionalizado del Estado británico. El SDS respondió en los años 80 y 90 espiando intensamente a estas comunidades. Recientemente se ha revelado que la SDS y la Unidad Nacional de Inteligencia para el Orden Público (NPOIU, por sus siglas en inglés) tenían como objetivo a las familias de las personas de color asesinadas por la policía[16]. La NPOIU también espió a la familia de Stephen Lawrence, que intentaba que se hiciera justicia después de que su hijo muriera en un ataque racista en Londres en los años 90. Su campaña atrajo la vigilancia de la policía después de que amenazara con sacar a la luz el racismo institucional de la Policía Metropolitana de Londres[17].

Policías encubiertos también se hicieron pasar por miembros de movimientos de acción directa ecologistas y de liberación animal a lo largo de la década de 1990, utilizando a menudo la táctica de entablar relaciones íntimas con mujeres organizadas políticamente para obtener información. Los agentes no revelaban su verdadera identidad a sus parejas[18]. Estas tácticas continuaron al menos hasta que se reveló el alcance del espionaje policial a finales de la década de 2000.

Las tácticas encubiertas se han utilizado junto con la vigilancia abierta de los movimientos sociales. En la década de 2000, la policía comenzó a utilizar en gran medida los Equipos de Inteligencia Avanzada (FIT), que seguían abiertamente a integrantes políticos, apareciendo a menudo con cámaras de largo alcance en

13 *PA News*, 2020, 'Shadowy police unit set up amid 1960s Vietnam war protests', ***Grampian Online***. https://www.grampianonline.co.uk/news/national/shadowy-police-unit-set-up-amid-1960s-vietnam-war-protests-5460/, [Accessed March 12 2021].

14 Undercover Research Group, November 2020, 'One hundred new political groups named as spycops targets' https://undercoverresearch.net/2020/11/02/more-groups-named-as-spycops-targets , [Accessed March 12 2021].

15 Undercover Research Group, June 2020, 'State Surveillance in 1984 – Union Organising as 'conspiracy', https://undercoverresearch.net/2020/01/06/state-surveillance-in-1984-trade-union-organising-as-conspiracy/ [Accessed March 12 2021].

16 Undercover Research Group, October 2019, 'How many black families were targeted by undercover officers?', https://undercoverresearch.net/2019/10/23/black-justice-campaigns/ [Accessed March 12 2021].

17 Evans, R. 2019, 'Black undercover officer who spied on Stephen Lawrence campaign named', ***The Guardian,*** https://www.theguardian.com/uk-news/2019/jul/16/black-undercover-officer-who-spied-on-stephen-lawrence-campaign-named, [Accessed March 12 2021].

18 Undercover Research Group, March 2019, "James Blond' - #spycop infiltrating animal right groups', https://undercoverresearch.net/2019/03/01/james-blond-spycop-infiltrating-animal-rights-groups/ [Accessed March 12 2021]. and Steel, H, 2014, 'I feel violated', ***The Guardian*** https://www.theguardian.com/uk-news/2014/aug/29/helen-steel-relationship-undercover-police-feel-violated [Accessed March 12 2021].

las protestas o reuniones políticas[19]. Según Richard Purssell, un integrante del movimiento antimilitarista al que los equipos FIT siguieron intensamente en las protestas antimilitaristas de Londres en 2009:

> *"**Están ahí para intimidarte y que no protestes**, para que no formes parte del pelotón de los incómodos. Hay un mensaje claro de que están por encima tuyo"*[20].

LEGISLACIÓN PARA ATACAR A LA DISIDENCIA

Los sucesivos gobiernos británicos han utilizado la legislación para criminalizar diferentes formas de disidencia que se consideran una amenaza para el status quo, y para criminalizar a determinadas comunidades. Los gobiernos conservadores de los años ochenta y noventa se centraron en el derecho a la huelga de los sindicalistas, establecieron poderes represivos de detención y registro dirigidos a las comunidades negras y musulmanas[21], e introdujeron una nueva Ley de Orden Público que incluía medidas destinadas específicamente a controlar las protestas políticas y a criminalizar a los ocupantes ilegales y a las comunidades nómadas[22].

En el año 2000, el gobierno laborista impulsó una represiva Ley de Terrorismo que, entre otros elementos profundamente preocupantes, ilegalizaba el apoyo a diversos grupos -incluidos los de izquierda- que Gran Bretaña considera terroristas. El apoyo se describió en los términos más amplios. Por ejemplo, la Ley tipifica como delito el uso de prendas de vestir que puedan indicar apoyo a alguno de los grupos incluidos en la lista[23]. Varias comunidades no blancas de Gran Bretaña -incluidos los partidarios de los movimientos por la liberación de las poblaciones tamil y kurda- se han enfrentado a la criminalización desde entonces[24].

19 Anderson, T. 2013, 'Chapter 16: "When Co-Option Fails" in Fisher, R. 'Managing Democracy, Managing Dissent', ***Corporate Watch,*** https://corporatewatch.org/wp-content/uploads/2017/09/MDMD-Master-PDF1.pdf [Accessed March 12 2021].

20 The Guardian, October 2009, 'Police spotter card G: Richard Purssell', https://www.theguardian.com/uk/2009/oct/27/police-spotter-card-richard-purssell [Accessed March 12 2021].

21 Casciani, D. 2002. 'Troubled history of stop and search', ***BBC News***, http://news.bbc.co.uk/1/hi/uk/2246331.stm [Accessed March 12 2021].

22 Anderson, T. 2013, 'Chapter 16: "When Co-Option Fails" in Fisher, R. 'Managing Democracy, Managing Dissent'.

23 CAMPACC: Campaign Against Criminalising Communities, 'Proscribed groups', Campacc.org.uk, http://campacc.org.uk/index.php?page-proscribed-groups[Accessed March 12 2021] and Gov.uk, 2000, 'Terrorism Act 2000' ***Legislation.gov.uk*** https://www.legislation.gov.uk/ukpga/2000/11/section/13 [Accessed March 12 2021].

24 CAMPACC: Campaign Against Criminalising Communities, 'Communities targeted for harassment and prosecutions', ***Campacc.org.uk*** http://campacc.org.uk/index.php?page-anti-terror-laws-and-communities [Accessed March 12 2021].

> Policía política – Anexo 7 de la Ley de Terrorismo

El Anexo 7 entró en vigor como parte de la Ley de Terrorismo del Reino Unido en el año 2000 y permite a la policía detener a personas a su llegada o salida del Reino Unido e interrogarlas para determinar si pueden estar implicadas en la organización de actos terroristas. A diferencia de otros poderes de interrogatorio policial, en virtud del Anexo 7 es ilegal responder "sin comentarios" o no responder. Las personas pueden ser detenidas, procesadas y encarceladas si se niegan a dar una respuesta. Aunque las preguntas tienen que estar relacionadas con la investigación del terrorismo, en realidad se ha interrogado a personas sobre una serie de temas no relacionados con las organizaciones "terroristas" proscritas. Por ejemplo, se ha interrogado a personas sobre sus creencias religiosas, su vida personal, su participación en protestas y su organización política, entre otros asuntos personales. En virtud del Anexo 7, la policía también está facultada para confiscar dispositivos electrónicos y exigir contraseñas, y tiene el poder de arrestar si estas no se facilitan[25].

Kevin Blowe, coordinador de la Red de Vigilancia Policial (NetPol), dijo a Shoal Collective:

> ***"El mayor uso del Anexo 7 es, sin duda, contra los musulmanes con opiniones políticas,*** *especialmente en cuestiones de política exterior o de seguridad. Es un poder policial fundamentalmente islamófobo. Sin embargo, como herramienta, este poder se dirige a la vigilancia de cualquier persona cuya política tenga la imaginación de mirar más allá de las fronteras: así, la solidaridad con los migrantes o las luchas independentistas, como la de los palestinos o los kurdos. Esto también implica reuniones de activistas de diferentes países que rechazan el papel del capitalismo en las soluciones al cambio climático, los conflictos o la pobreza global. Por eso es imposible ver el uso del Anexo 7 como algo distinto a una flagrante labor de policía política"*[26].

La Ley de Regulación de los Poderes de Investigación de 2000 incrementó los poderes de vigilancia policial encubierta y tipificó como delito no revelar a la policía las contraseñas de los dispositivos electrónicos en determinadas circunstancias[27].

La policía británica comenzó a utilizar el término *"extremismo doméstico"* durante la década de 2000 para describir a los partidarios de los movimientos de izquierda, las campañas de acción directa, los grupos de protesta y la extrema derecha. Los apodados *"extremistas domésticos"* han sido sometidos a una exce-

25 Gov.uk, 2000, 'Terrorism Act 2000' Legislation.gov.uk and Gov.uk, 2000, 'Schedule 7', Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2000/11/schedule/7 [Accessed March 12 2021] and Cooper, T and Anderson, T, February 2013, 'Schedule 7 of the Terrorism Act 2000: A police snooping tool to protect private profit', ***Corporate Occupation***, https://corporateoccupation.org/2013/02/27/schedule-7-of-the-terrorism-act-2000-a-police-snooping-tool-to-protect-private-profit/ [Accessed March 12 2021].

26 Quote given to Shoal Collective by Kevin Blowe, coordinator of Network for Police Monitoring, 2020.

27 Gov.uk, 2000, 'Regulation of Investigatory Powers Act 2000', Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed March 12 2021].

siva vigilancia policial[28] y han sido denigrados en los medios de comunicación. Según Netpol, la etiqueta tiene un efecto ***"escalofriante"*** sobre ***"la participación en protestas y campañas públicas"*** y limita ***"los valores fundamentales que se encuentran en el corazón de una sociedad justa y libre"***[29].

El programa PREVENT del gobierno laborista[30] llevó la vigilancia estatal en Gran Bretaña a un nuevo nivel profundamente preocupante. Se hizo obligatorio que los funcionarios, como los profesores, los profesionales de la medicina y otros empleados del Estado, informaran a las autoridades de cualquier comportamiento que consideraran sospechoso, bajo la lógica de que al hacerlo podrían adelantarse a un inminente ataque terrorista[31]. La ley PREVENT fue reforzada por los sucesivos gobiernos conservadores[32] y, hoy en día, la ley PREVENT impone a los funcionarios la obligación de espiar y denunciar a las personas en entornos como escuelas y universidades, durante las citas médicas o mientras están en el hospital. Según Netpol, PREVENT ***"criminaliza la disidencia legítima mediante la recopilación de información sobre los pensamientos y creencias de personas que no están involucradas en actividades delictivas"***[33].

Los poderes draconianos de PREVENT se vieron reforzados por la Ley de Seguridad y Lucha contra el Terrorismo del gobierno conservador, aprobada en 2015[34]. Esta ley también obligó -en muchos casos- a los proveedores de servicios de comunicación a conservar y entregar información sobre las direcciones de protocolo de Internet (IP) de los usuarios, lo que facilita la vinculación de las personas con dispositivos electrónicos y ubicaciones concretas[35].

28 Network for Police Monitoring, January 2020, 'Domestic Extremism', Netpol.org, https://netpol.org/domestic-extremism/ [Accessed March 12 2021].

29 *Ibid.*

30 Full Fact, August 2017, 'What is the Prevent strategy?', Fullfact.org, https://fullfact.org/law/what-prevent-strategy/ [Accessed March 12 2021].

31 Gov.uk, 2019, 'Revised Prevent duty guidance: for England and Wales', https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales [Accessed March 12 2021].

32 Network for Police Monitoring, June 2018, 'PREVENT', Netpol.org, https://netpol.org/campaigns/prevent/ [March 12 2021] and Economic and Social Research Council, August 2015, 'PREVENT', Esrc.ukri.org, https://esrc.ukri.org/public-engagement/social-science-for-schools/resources/prevent-the-uk-s-counter-terrorism-strategy/ [Accessed March 12 2021].

33 Network for Police Monitoring, June 2018, 'PREVENT', Netpol.org.

34 Gov.uk, 2015, 'Counter Terrorism and Security Bill', Legislation.gov.uk, https://www.gov.uk/government/collections/counter-terrorism-and-security-bill [Accessed March 12 2021].

35 Home Office, July 2016, 'Counter Terrorism and Security Bill', Gov.uk, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/540538/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf [Accessed March 12 2021].

> La Ley de Poderes de Investigación; un mandato para un Estado de vigilancia

En diciembre de 2016, el Parlamento británico aprobó la Ley de Poderes de Investigación[36], que otorga a las fuerzas policiales y a los agentes de inteligencia el derecho legal a ***"hackear ordenadores, redes, dispositivos móviles, servidores... Esto podría incluir la descarga de datos de un teléfono móvil robado o dejado sin vigilancia, o la instalación en un ordenador portátil de un software que rastrea cada letra del teclado que se pulsa"***[37]. Apodada como "carta de los fisgones"[38], muestra hasta dónde está dispuesto a llegar el gobierno británico para espiar a la población británica, en particular a los participantes de movimientos sociales, periodistas y abogados que actúan en su nombre. La organización de derechos civiles Liberty declaró que la Ley de Poderes de Investigación permite al gobierno ***"espiar a cada uno de nosotros, violando nuestros derechos a la privacidad y a la libre expresión"***[39].

El gobierno respondió a la crisis sanitaria del Covid-19 aprobando una Ley sobre el Coronavirus. Se supone que la Ley sólo está en vigor temporalmente[40], pero Big Brother Watch ha calificado sus restricciones como los "***poderes más draconianos que jamás haya tenido Gran Bretaña en tiempos de paz"***[41]. La Ley se ha utilizado ampliamente para prohibir las protestas y detener a los manifestantes[42]. Mientras tanto, las fuerzas policiales han incrementado la vigilancia durante el Covid-19 aumentando masivamente el uso de drones de vigilancia[43], mientras que los datos de la aplicación NHS Test and Trace -que ha sido descargada por más de 20 millones de personas[44]- también se han puesto a disposición de la policía[45].

36 UK Parliament, 2017, Parliament.uk https://publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf [Accessed March 12 2021].

37 Burgess, M. 2017, 'What is the IP Act and how will it affect you?', ***Wired UK***, https://www.wired.co.uk/article/ip-bill-law-details-passed [Accessed March 12 2021].

38 Griffin, A. 2016, 'Britain just got perhaps the most intrusive spying powers ever seen', ***The Independent***, https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html [Accessed March 12 2021].

39 Perraudin, F, July 2019, 'Liberty loses high court challenge to snooper's charter', ***The Guardian***, https://www.theguardian.com/law/2019/jul/29/liberty-loses-high-court-challenge-to-snoopers-charter [Accessed March 12 2021].

40 Big Brother Watch, February 2021, 'Emergency Powers and Civil Liberties report, February 2021', ***Bigbrotherwatch.org***, https://bigbrotherwatch.org.uk/wp-content/uploads/2021/03/Emergency-Powers-and-Civil-Liberties-Report-FEB-2021.pdf [Accessed March 16 2021], Page 8.

41 Big Brother Watch website homepage, 2021, ***Bigbrotherwatch.org,*** https://bigbrotherwatch.org.uk/ [accessed 16 March 2021].

42 Anderson, T, September 2020, 'The British police are using Covid-19 measures to criminalise dissent, we need to fight back', ***The Canary,*** https://www.thecanary.co/opinion/2020/09/09/the-british-police-are-using-covid-19-measures-to-criminalise-protest-we-need-to-be-ready-to-fight-back/ [Accessed 16 March 2021].

43 See Chapter 2.

44 Mageit, S, January 2021, 'UK Government Reports Test and Trace reaching record number of people', Healthcare IT News, https://www.healthcareitnews.com/news/emea/uk-government-reports-nhs-test-and-trace-reaching-record-number-people [Accessed 16 March 2021].

45 BBC News, October 2020, 'Coronavirus: Police get access to NHS Test and Trace self-isolation data', ***BBC News,*** https://www.bbc.co.uk/news/uk-54586897 [accessed 16 March 2021].

En el momento de la redacción de este informe, se estaban llevando a cabo protestas contra el proyecto de ley de 2021 sobre policía, delincuencia, sentencias y tribunales. Si se aprueba, esta ley supondrá la mayor represión de la libertad de protesta en el Reino Unido desde la Ley de Orden Público. La propuesta consiste en modificar la Ley de Orden Público otorgando a la policía mayores poderes para imponer restricciones a las reuniones públicas, detener a los manifestantes en función del ruido que hacen, criminalizar la entrada ilegal y ampliar los poderes de detención y registro. Se endurecerán las penas por agredir a los policías y se creará un nuevo delito de alteración del orden público, castigado con hasta diez años de cárcel[46].

El proyecto de ley amenaza con criminalizar aún más a las comunidades de gitanos, romaníes y nómadas del Reino Unido, que podrían ser procesadas o encarceladas por montar campamentos en terrenos de propiedad privada[47]. El colectivo No Fixed Abode Travellers and Supporters hizó la siguiente declaración:

> *"Es un hecho que nuestro derecho absoluto como seres humanos a viajar de forma nómada está siendo cuestionado y esto no está bien. Nadie debería ser cuestionado, controlado, arrestado o tener sus casas confiscadas por elegir un estilo de vida nómada."*[48]

El proyecto de ley también está concebido como una respuesta autoritaria al movimiento Black Lives Matter, que derribó estatuas que conmemoran la historia racista de Gran Bretaña. Propone que el daño a los monumentos nacionales se castigue con hasta diez años de prisión[49].

46 Norden. J. March 2020, 'Pritti Patel's new policing bill is threatening our right to protest', The Canary, Disponible en: https://www.thecanary.co/uk/analysis/2021/03/15/priti-patels-new-policing-bill-is-threatening-our-right-to-protest/ [Accessed March 12, 2021].

47 Lally, K. March 2021, Travellers could be imprisoned for setting up camps under new government bill, Liverpool Echo, https://www.liverpoolecho.co.uk/news/liverpool-news/travellers-could-imprisoned-setting-up-20190702 [Accessed 17 March 2021].

48 No Fixed Abode Travellers and Supporters, Undated, 'Campaigns', https://nfats1.wixsite.com/nfatscollective/campaigns [Accessed 17 March 2021].

49 UK Parliament, 2021, 'Police, Crimes, Sentencing and Courts Bill, Parliament.uk, https://publications.parliament.uk/pa/bills/cbill/58-01/0268/200268.pdf [Accessed March 16 2021].

VISTO BUENO A UNA MAYOR VIGILANCIA

Al mismo tiempo que se leía el proyecto de ley en el Parlamento, se publicó un informe de la Inspección de la Policía de Su Majestad (HMIC, por sus siglas en inglés) en el que se hacían una serie de recomendaciones, entre las que se proponía el uso continuado de tecnologías de vigilancia de alto nivel, como el reconocimiento facial y los drones, contra los manifestantes[50]. El informe también establece una estrategia para una nueva era de vigilancia policial, a través del equipo de Inteligencia e Información Estratégica del Centro Nacional de Coordinación Policial (NPoCC SIB). El NPoCC SIB recopilará información de las diferentes fuerzas policiales sobre la disidencia en el Reino Unido, y ***"asumirá la responsabilidad nacional de la inteligencia relacionada con las protestas"***[51].

Según Kevin Blowe, de Netpol, el informe:

> *"da luz verde a una mayor vigilancia de los activistas, así como a la creación de una nueva etiqueta: "activistas agravados". En esencia, resucita la Unidad Nacional de Inteligencia para el Orden Público, la desprestigiada unidad de vigilancia de las protestas que empleaba agentes encubiertos"*[52].

El gobierno conservador también está tratando de impulsar otro proyecto de ley que autorizará a agentes encubiertos, como policías, agentes del MI5 o personal militar, a llevar a cabo de manera legal lo que normalmente se consideraría una conducta delictiva. El proyecto de ley sobre fuentes de inteligencia humana encubiertas daría a los policías encubiertos el visto bueno para seguir engañando a las mujeres para que mantengan relaciones sexuales[53].

50 Her Majesty's Inspectorate of Constabulary (HMIC), March 2021, 'Getting the balance right? An inspection of how effectively the police deal with protests', ***Justiceinspectorates.gov.uk,*** https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/getting-the-balance-right-an-inspection-of-how-effectively-the-police-deal-with-protests.pdf [Accessed 11 March 2020].

51 ***Ibid***, page 7.

52 Cita obtenida por teléfono de Kevin Blowe de Netpol por Shoal Collective, 17 de marzo de 2020.

53 Egret, E. January 2021, 'The most dangerous law of our time continues to be pushed through parliament', ***The Canary,*** https://www.thecanary.co/uk/analysis/2021/01/13/the-most-dangerous-law-of-our-time-continues-to-be-pushed-through-parliament/ [Accessed 16 March 2021].

LA VIGILANCIA MASIVA SE BURLA DE LA LEY DE DERECHOS HUMANOS

El modelo de vigilancia masiva profundamente invasivo que se utiliza para vigilar y controlar a comunidades enteras se burla de las normas de derechos humanos que el Estado dice defender y proteger. El artículo 8 de la Ley de Derechos Humanos del Reino Unido incluye el derecho a la confidencialidad de la información privada y el derecho a no ser sometido a vigilancia estatal ilegal[54], pero la nueva tecnología desplegada por el Estado se burla de estos "derechos" y permite la vigilancia masiva a un nivel sin precedentes. En 2020, el gobierno conservador de Boris Johnson anunció planes para derogar la Ley de Derechos Humanos del Reino Unido tras la salida de este país de la Unión Europea[55]. Actualmente se está llevando a cabo una revisión de la ley[56]. La derogación de la Ley eliminaría muchas protecciones legales y daría rienda suelta a la expansión del estado de vigilancia.

54 Liberty, Undated, 'A private and family life',***Libertyhumanrights.org.uk***, https://www.libertyhumanrights.org.uk/right/a-private-and-family-life/ [Accessed March 12 2021].

55 Boffey, D. October 2020, 'Boris Johnson set for compromise on Human Rights Act – EU sources', ***The Guardian***, https://www.theguardian.com/politics/2020/oct/07/boris-johnson-set-to-make-compromise-on-human-rights-act-eu-source [Accessed March 12, 2021].

56 Allen, K, 2021, 'The government is hell-bent on diluting the Human Rights Act. We must protect it', ***MSN***, https://www.msn.com/en-gb/news/other/the-government-is-hell-bent-on-diluting-the-human-rights-act-we-must-protect-it/ar-BB1ec8G6 [Accessed March 12 2021].

Vigilancia de Estado: El caso de Reino Unido

2 TECNOLOGÍAS DE VIGILANCIA

En este capítulo se analiza cómo la tecnología permite al Estado británico vigilar en masa a su población de modos nunca vistos.

HACKING GUBERNAMENTAL

En 2013, el denunciante Edward Snowden reveló que la agencia de inteligencia, cibernética y de seguridad del Reino Unido, conocida como el Cuartel General de Comunicaciones del Gobierno (GCHQ), intervenía los cables de fibra óptica para recopilar enormes cantidades de datos personales de los usuarios de Internet a través de su sistema informático Tempora. Estos datos también se compartían con la Agencia de Seguridad Nacional de Estados Unidos (NSA) [57]. Tempora intercepta las llamadas telefónicas y accede a los datos del teléfono[58], y la filtración de Snowden reveló que el GCHQ se aprovechó de las aplicaciones telefónicas "filtradas" para acceder a información sobre la edad, el sexo y la ubicación de los usuarios del teléfono[59]. La agencia también puede activar el teléfono de una persona mientras está apagado, y encender el micrófono de un dispositivo para escuchar las conversaciones[60]. El GCHQ ha interceptado los datos de los usuarios en su paso por los servidores de Google y ha espiado a 1,8 millones de usuarios de cámaras web, guardando imágenes de sus conversaciones[61].

57 MacAskill, E. Borger, J. Hopkins, N. Davies, N. Ball, J. June 2013, 'GCHQ taps fibre-optic cables for secret access to world's communications', ***The Guardian***, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed March 12 2021].

58 Gallagher, R. 2014, 'The Inside Story of How British Spies Hacked Belgium's Largest Telco', ***The Intercept***, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ [Accessed March 12 2021].

59 Ball, J. 2014, 'Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data', ***The Guardian*** , https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed March 12 2021].

60 Amnesty International, 2015, 'Ten Spy programmes with silly codenames used by GCHQ and NSA'. ***Amnesty.org,*** https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/ [Accessed March 12 2021].

61 ***Ibid.***

RECOGIDA POLICIAL DE DATOS DE DISPOSITIVOS INCAUTADOS

Cuando se detiene a una persona, ya sea en las fronteras del Reino Unido o mediante arresto domiciliario, la policía suele incautar teléfonos, tabletas, ordenadores, tarjetas de memoria y tarjetas SIM, para extraer datos personales. Varias empresas suministran equipos a la policía del Reino Unido para ello, como Cellebrite, Digital Detective, ElcomSoft, Grayshift, Magnet Forensics, MSAB, OpenText y Oxygen Forensics[62].

Varias fuerzas policiales del Reino Unido utilizan la tecnología desarrollada por la empresa israelí Cellebrite para desbloquear y extraer datos de los teléfonos inteligentes[63], lo que les permite descifrar contraseñas y extraer listas de contactos, historial de llamadas, historial de Internet, entradas del calendario, correos electrónicos, mensajes SMS, documentos, fotos y vídeos, así como ver qué aplicaciones se utilizaron y los datos almacenados en ellas. La tecnología de Cellebrite también permite a las fuerzas policiales obtener información sobre la ubicación, así como recuperar archivos ocultos y contenidos borrados.

En 2018, Privacy International informó de que más de la mitad de las fuerzas policiales del Reino Unido habían confirmado que utilizaban tecnología de extracción de teléfonos móviles[64], mientras que en Escocia, la cooperativa de medios The Ferret reveló en 2017 que "en los últimos tres años la Policía de Escocia ha conseguido obtener datos de al menos 35.973 teléfonos. En el mismo periodo la policía se hizo con 16.587 ordenadores"[65].

62 MSAB company website: https://www.msab.com/company, https://www.msab.com/products/xry/, https://www.msab.com/products/xry/xry-cloud/, Digital Detective company website: https://www.digital-detective.net/about-us/executive-team/, ElcomSoft company website: https://www.elcomsoft.co.uk/company.html, Oxygen Forensics company website: https://www.oxygen-forensic.com/en/company, GrayShift company website: https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk, Magnet Forensics company website: https://www.magnetforensics.com/for-police-leaders all undated and [accessed March 16 2021] and Scottish Parliament Reports. 2019, 'Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks)', https://digitalpublications.parliament.scot/Committees/Report/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-#Digital-device-triage-systems---cyber-kiosks [Accessed 16 March 2021].

63 Cellebrite, Undated, 'Cellebrite Mobile Forensics Tool Demonstration', Youtube.com, https://www.youtube.com/watch?v=5fEYqpJ6Mrw [Accessed March 12 2021] and Privacy International, April 2020, 'Are UK police accessing your cloud apps?', Privacyinternational.org, https://privacyinternational.org/report/3551/are-uk-police-accessing-your-cloud-apps [Accessed March 12 2021].

64 Privacy International, March 2018, 'Digital stop and search: how the UK police can secretly download everything from your mobile phone', ***Privacyinternational.org***, https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile [Accessed March 12 2021].

65 Tibbitt, A, 2017, 'Everything Police Scotland can find out about you from your mobile phone'. ***The Ferret***, https://theferret.scot/privacy-mobile-phones-cellebrite-police-scotland/ [Accessed March 12 2021] and ***Freedom of Information*** (FOI) request made by The Ferret in March 2017 https://www.documentcloud.org/documents/3938332-17-0297-Final-Response.html [Accessed March 12 2021].

EXTRACCIÓN DE DATOS DE SERVIDORES DE TERCEROS

La tecnología de extracción en la nube está diseñada para extraer datos personales almacenados en servidores de terceros como Dropbox, Slack, Instagram, Twitter y Facebook, My Activity, Uber y Hotmail. Privacy International describe la tecnología de extracción en la nube como la ***"tecnología secreta que permite a las agencias gubernamentales recopilar grandes cantidades de datos de tus aplicaciones"***[66].

La compañía Cellebrite afirma en un vídeo de promoción de su tecnología de computación en la nube Universal Forensic Extraction Device (UFED) que, mediante el uso de su software UFED Cloud, se puede "***acceder a datos que ya no residen en el dispositivo físico recuperando copias de seguridad en la nube. Además, UFED Cloud permite ver la actividad digital de un usuario y sus ubicaciones en múltiples dispositivos, ordenadores y tablas de fuentes en la nube como Facebook, iCloud y Google***"[67]. La tecnología de Cellebrite también tiene la capacidad de utilizar el reconocimiento facial al analizar las fotos extraídas del almacenamiento en la nube[68].

Privacy International explica que esta tecnología permite a la policía rastrear continuamente a alguien. "***Al adquirir las credenciales de acceso, permite a sus usuarios seguir rastreando el comportamiento en línea del usuario del dispositivo, aunque ya no esté en posesión del teléfono***"[69]. Además, "el propio individuo nunca sabrá que alguien tiene acceso a su perfil en la nube y puede estar utilizándolo"[70]. Privacy International también señala que con el acceso a los datos de alguien o a sus cuentas en la nube, es posible suplantar su identidad y enviar mensajes como si fueran del propietario del dispositivo[71].

66 Privacy International, January 2020, 'Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps', Privacyinternational.org, https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data [Accessed March 12 2021].

67 Cellebrite, Undated, Cellebrite.com, www.cellebrite.com/en/ufed-cloud-analyzer-5/ [Accessed October 2020] and Cellebrite's YouTube channel: https://www.youtube.com/watch?v=dJbl8Tiz3-k [Accessed March 12 2021].

68 Privacy International, January 2020, 'Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps'.

69 *Ibid.*

70 *Ibid.*

71 *Ibid.*

ESPIONAJE DE LA MENSAJERÍA SEGURA

Varias empresas anuncian la posibilidad de espiar servicios de mensajería segura como Signal y Telegram. La empresa rusa ElcomSoft, por ejemplo, afirma que su tecnología puede ***"permitir a los expertos acceder a información protegida por contraseña, bloqueada y encriptada que esté contenida en una serie de dispositivos móviles y servicios en la nube"***[72]. La tecnología Phone Viewer 5.0 de ElcomSoft puede, en teoría, ver las conversaciones de mensajería privada de Telegram y Signal[73]. Entre sus clientes figuran varias fuerzas policiales, así como la Oficina de Fraudes Graves y el Ministerio de Defensa[74].

MONITORIZACIÓN DE LAS COMUNICACIONES

Un IMSI-catcher es una herramienta de vigilancia masiva que utiliza la policía para controlar los teléfonos. Se hace pasar por una torre de telefonía móvil a la cual pueden conectarse los teléfonos de forma automática o sin saberlo, pero al hacerlo, el número IMSI -International Mobile Subscriber Identity-, que es único para cada tarjeta SIM, queda registrado y puede ser utilizado por la policía para rastrear la identidad del propietario del teléfono[75].

Según Privacy International: "Los IMSI-catchers son herramientas de vigilancia indiscriminada que podrían utilizarse para rastrear quién asiste a una manifestación política o a un evento público como un partido de fútbol. Incluso pueden utilizarse para vigilar tus llamadas y editar tus mensajes, sin que te des cuenta"[76]. Además, The Intercept descubrió que los IMSI-catchers pueden instalar potencialmente malware en el teléfono de una persona[77].

A finales de 2015, VICE News y Privacy International detectaron el uso de un captador IMSI en una protesta contra la austeridad en Londres. Cuando se le preguntó al respecto, un agente de policía que se encontraba en el lugar de los hechos dijo que "no podía confirmar ni negar" su uso[78]. Posteriormente, Vice y Privacy International enviaron solicitudes de información a las fuerzas policiales de todo el Reino Unido, y todas ellas se negaron a confirmar si utilizaban los

72 ElcomSoft, Undated, https://www.elcomsoft.co.uk/company.html, Elcomsoft.co.uk, [Accessed March 12 2021].

73 ElcomSoft, Undated, 'Phone Viewer 5.0 gains the ability to display conversation histories and secret chats in Telegram - Help Net Security. Help Net Security', https://www.helpnetsecurity.com/2020/04/30/elcomsoft-phone-viewer-5-0/ [Accessed March 12 2021].

74 ElcomSoft, Undated, https://www.elcomsoft.co.uk/company.html, Elcomsoft.co.uk.

75 Privacy International, August 2018, 'IMSI Catchers', Privacyinternational.org, https://www.privacyinternational.org/explainer/2222/imsi-catchers [Accessed March 12 2021].

76 Privacy International, August 2018, 'IMSI Catchers', Privacyinternational.org.

77 Zetter, K. 2020, 'What Are Stingrays and Dirtboxes?', ***The Intercept***, https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [Accessed March 12, 2021].

78 Vice News, 2016, 'Phone Hackers: Britain's Secret Surveillance', Vice.com, https://www.vice.com/en/article/9kjxe7/phone-hackers-britains-secret-surveillance [Accessed March 12 2021].

IMSI-catchers. Sin embargo, The Bristol Cable descubrió que, en 2015, la Policía Metropolitana de Londres pagó más de un millón de libras esterlinas a CellXion, que fabrica los IMSI-catchers. El pago fue por la tecnología de captura de datos de comunicaciones encubiertas (CCDC). La policía de Avon y Somerset y la de West Midlands también compraron tecnología CCDC a CellXion[79]. Otras investigaciones de The Bristol Cable han revelado que al menos nueve fuerzas policiales del Reino Unido han comprado IMSI-catchers. Otra solicitud en virtud de la Libertad de Información (FOI) realizada por The Ferret en 2016 reveló que el Servicio Penitenciario Escocés (SPS) había estado utilizando IMSI-catchers para bloquear las llamadas salientes de los presos[80].

LA BÚSQUEDA FACIAL Y LA BASE DE DATOS NACIONAL DE LA POLICÍA

Todas las fuerzas policiales del Reino Unido, así como otros organismos gubernamentales, pueden buscar en la Base de Datos Nacional de la Policía (PND) mediante una herramienta de "búsqueda facial", que se basa en la tecnología de reconocimiento facial (FRT)[81]. La PND contiene más de 3.500 millones de registros policiales locales[82] y cada mes se cargan unas 100.000 imágenes nuevas[83]. El uso del PND se rige por la Ley de Protección de Datos y la Ley de Derechos Humanos, y se supone que la policía sólo puede utilizarlo para investigar o prevenir delitos penales o civiles. En la práctica, sin embargo, estos poderes pueden interpretarse de forma muy amplia[84]. La "búsqueda facial" permite a la policía y a otros organismos estatales buscar fotografías en el PND de personas que han sido detenidas en el Reino Unido, incluso de personas que nunca han sido condenadas por ningún delito[85]. Esta tecnología permite a la policía cotejar las imágenes de las cámaras de seguridad con las imágenes almacenadas en el PND utilizando la FRT[86]. La puesta a disposición del FRT a través de la citada base de datos ha costado al Ministerio del Interior británico -es decir, a los

79 Aviram A. 2016, 'Revealed: Bristol's police and mass mobile phone surveillance', ***The Bristol Cable,*** https://thebristolcable.org/2016/10/imsi/ [Accessed March 12 2021].

80 Rigg. J. May 2017, 'Stringray phone tracker use in the UK admitted for the first time', ***Engadget.com,*** https://www.engadget.com/2016-05-27-stringray-phone-tracker-uk.html?guce_referrer=aHR0cHM6Ly9kdW/NrZHVja2dvLmNvbS8_cT1IYXJyaXMrc3RpbmdyYXkrVXNlK2luK1VLJnQ9bG0maWEgd2Vi&guce_referrer_sig=AQAAALgfOke7VVDu8-oBzRCYZFG1Wnui3B7QGtUlDr3NMYikFZr6B4iv0lkEv55HozGK497J3pG4KFkCnLyERHf-Fo7drn2rRWQWAOagVQUn53cTLZiFxOLORJpaaSkcJmf1SOJzKx6SERjMkfkidaddblbzJ7l3pP6ofkxGLhRtETfl&guccounter=2 [Accessed March 12 2021] and Aviram, A. 2016, ***'IMSI catchers: a campaign for police to come clean on mass mobile phone surveillance', The Bristol Cable,*** https://thebristolcable.org/imsi/ [Accessed 16 March 2021].

81 Home Office, 2019, 'Team H. Fact Sheet on live facial recognition used by police', Homeofficemedia.blog.gov.uk, https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/ [Accessed March 12 2021].

82 Babuta. A, September 2020, 'Big Data and Policing', ***Rusi.org***, https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf [Accessed March 12 2021].

83 Solicitud FOI realizada por Pippa King al Ministerio del Interior en 2015, https://www.whatdotheyknow.com/request/263544/response/665587/attach/2/20150616%20Response%20Letter%2035046.pdf [Accessed 16 March 2021].

84 Gov.uk, 2010, 'On the Operation and Use of the Police National Database. National Policing and Improvement Agency', Gov.uk, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243554/9999102808.pdf [Accessed March 16. 2021.

85 BBC News, September 2017, 'Facial recognition database 'risks targeting innocent people'. ***BBC News***, https://www.bbc.co.uk/news/amp/uk-41262064 [Accessed March 12 2021].

86 Babuta. A, September 2020, 'Big Data and Policing', Rusi.org.

contribuyentes- 1,1 millones de libras[87]. Según el Ministerio del Interior, las empresas privadas que gestionan el PND sólo tienen acceso al software de la base de datos, pero no a su contenido.

RECONOCIMIENTO FACIAL RETROSPECTIVO

Seis fuerzas policiales del Reino Unido utilizan el "reconocimiento facial retrospectivo"[88]. Según el HMIC, este método:

> *"utiliza las imágenes captadas por una cámara, comparándolas posteriormente con una gran base de datos de imágenes faciales que posee la policía para tratar de identificarlas"*[89].

El "reconocimiento facial retrospectivo" permite a la policía comparar las imágenes con bases de datos distintas de la PND.

EL USO DEL RECONOCIMIENTO FACIAL EN VIVO POR PARTE DE LAS FUERZAS POLICIALES DEL REINO UNIDO

El reconocimiento facial en vivo (LFR) es la aplicación en tiempo real del FRT. Según la revista Science Focus: "El reconocimiento facial en vivo (LFR), también conocido como reconocimiento facial automático, identifica a las personas en un vídeo en tiempo real, utilizando un conjunto de fotografías como referencia. Cuando se utiliza en público, las cámaras escanean una multitud y el software destaca cualquier coincidencia entre los miembros del público y las personas de su base de datos"[90].

Actualmente, sólo cinco fuerzas policiales del Reino Unido utilizan el LFR, mientras que 25 fuerzas tienen previsto probar esta tecnología[91]. La Policía de Gales del Sur y la Policía Metropolitana de Londres son las que más han probado esta tecnología:

La Policía de Gales del Sur ha utilizado el LFR en 61 ocasiones desde 2017 en conciertos, en centros comerciales, en eventos deportivos y en al menos una protesta política[92]. En 2018, detuvo a 22 personas tras ser identificadas a través de

87 Solicitud FOI realizada por Pippa King al Ministerio del Interior en 2015, https://www.whatdotheyknow.com/request/263544/response/665587/attach/2/20150616%20Response%20Letter%2035046.pdf [Accessed March 16 2021].

88 *HMIC,* 'Getting the balance right', 2021, Page 47.

89 *Ibid.*

90 Rigby, S., 2019. ***Live facial recognition: how is it used? BBC Science Focus Magazine,*** https://www.sciencefocus.com/future-technology/live-facial-recognition-how-is-it-used/ [Accessed 16 March 2021]

91 *HMIC,* 'Getting the balance right', 2021, Page 47.

92 South Wales Police, Undated, 'Court of Appeal Judgment', Afr.south-wales.police.uk, https://afr.south-wales.police.uk/blog/court-of-appeal-judgment/ [Accessed March 12 2021].

LFR[93]. El software LFR lo proporciona el gigante japonés de la electrónica NEC[94].

La Policía Metropolitana afirma que utiliza la tecnología NeoFace LFR de NEC[95], y que ha utilizado LFR en al menos 17 ocasiones entre 2016 y 2020, incluso en las concurridas calles comerciales de Oxford Circus[96], en el centro de Romford y en los alrededores del centro comercial Westfield de Stratford[97].

El LFR también ha sido utilizado por la policía de Hull, Leicestershire y Liverpool, y en lugares públicos como los muelles de Hull y el Download Music Festival, donde se cotejaron 90.000 personas con la base de datos de Europol en toda la UE[98].

Según Big Brother Watch, la policía ha apoyado la puesta a prueba de equipos de reconocimiento facial en Birmingham, Bradford, Brighton y Manchester y en zonas propiedad de empresas privadas, como centros comerciales, un estadio de fútbol, un centro de conferencias y un museo[99].

RECONOCIMIENTO AUTOMÁTICO DE MATRÍCULAS (RAM)

La policía del Reino Unido lleva utilizando la tecnología de reconocimiento automático de matrículas (RAM) desde los años 90[100], y el sistema se ha implantado en todo el país desde 2006[101]. Las fuerzas policiales tienen acceso a las imágenes de una red de 14.000 cámaras[102] que producen 50 millones de "registros de lectura" RAM al día. El Ministerio del Interior adjudicó recientemente un contrato al gigante armamentístico multinacional BAE Systems para suministrar un nuevo Sistema Nacional de RAM, con un coste de 14 millones de libras. El sistema entrará en funcionamiento en 2019[103].

93 South Wales Police, Undated, 'What is AFR?', Afr.south-wales.police.uk, https://afr.south-wales.police.uk/ [Accessed March 12 2021].

94 South Wales Police, Undated, 'Home', Afr.south-wales.police.uk, https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/ [Accessed March 12 2021].

95 Metropolitan Police, 2021, 'Update on facial recognition', Met.police.uk, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition-trial/ [Accessed 16 March 2021].

96 Solicitud FOI a la Policía Metropolitana en febrero de 2020, https://www.whatdotheyknow.com/request/648561/response/1610448/attach/5/20%2003%2006%20LFR1%20URN%202020%20002%20BOOTH%20FOIA%20REDACTED%20WAD%20Q1.PDF.pdf?cookie_passthrough=1

97 Vincent, J. 2020, 'London police to deploy facial recognition cameras across the city', *The Verge* https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment [Accessed 16 March 2021].

98 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk, https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ [Accessed 16 March 2021].

99 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk.

100 Big Brother Watch, Undated, 'Police use of ANPR', Bigbrotherwatch.org, https://bigbrotherwatch.org.uk/wp-content/uploads/2013/03/ANPR-Report.pdf [Accessed 16 March 2021].

101 The Independent, 2005. '*Surveillance UK: why this revolution is only the start', Independent Online Edition, Science & Tech,* https://web.archive.org/web/20080103025848/ http://news.independent.co.uk/sci_tech/article334684.ece [Accessed 16 March 2021].

102 Trendall, S. 2018. 'Home Office rolls on with £14m project to replace police number-plate database', https://publictechnology.net/articles/news/home-office-rolls-%C2%A314m-project-replace-police-number-plate-database [Accessed 16 March 2021].

103 BAE Systems, 2020, 'Transforming nationwide automatic number plate recognition, https://www.baesystems.com/en/cybersecurity/feature/transforming-nationwide-automatic-number-plate-recognition-anpr, [Accessed 16 March 2021].

DRONES

La policía británica se sirve de pequeños drones por control remoto desde noviembre de 2015, cuando fueron utilizados conjuntamente por la Policía de Devon y Cornualles y la Policía de Dorset[104]. Se emplean cada vez más para la vigilancia en operaciones de búsqueda y rescate y en la supervisión de escenas de delitos, pero también sirven para vigilar las protestas políticas[105], y se están desplegando regularmente para supervisar los encierros ocasionados por la pandemia del COVID-19[106]. La mitad de las fuerzas policiales del Reino Unido utilizan, según se informa[107], drones, muchos de ellos a diario[108], y muchos utilizan drones equipados con tecnología de imagen térmica.

Según las cifras obtenidas en virtud de la FOI de la policía de Avon y Somerset, hubo un aumento del 47,3% en el uso de drones por parte de las fuerzas de seguridad durante el período de marzo a junio de 2020, durante el primer bloqueo del Coronavirus en el Reino Unido, en comparación con el periodo de marzo a junio de 2019. Las fuerzas del orden utilizaron drones en 103 ocasiones en los primeros seis meses de 2020, lo que significa que los vuelos tuvieron lugar casi a diario[109]. Este aumento se debió probablemente a las medidas de aplicación del bloqueo. La Policía de Gales del Sur también informó de un aumento sustancial en el uso de drones durante el primer encierro por COVID-19, en comparación con los meses anteriores[110]. La policía de Derbyshire utilizó polémicamente un dron para avergonzar a las personas que paseaban a sus perros en el Distrito de Peak durante el confinamiento[111], mientras que la policía de Surrey reprodujo un mensaje grabado desde un dron, ordenando a los grupos que se dispersaran durante el fin de semana de Pascua de 2020[112]. La policía de West Midlands y la del Gran Manchester utilizaron drones equipados con cámaras térmicas para vigilar las fiestas ilegales durante agosto de 2020[113].

104 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics*** Home, https://www.politicshome.com/news/article/military-grade-drones-home-office [Accessed 16 March 2021].

105 HMIC, 'Getting the balance right', 2021, Page 42.

106 Solicitud FOI realizada por Tom Anderson a la policía de Kent en julio de 2020. https://www.whatdotheyknow.com/request/676655/response/1616941/attach/html/4/20%2007%200870%20Appendix.xlsx.html [Accessed 16 March 2021].

107 Heliguy, 2018. 'Drones a game-changer, say police', Heliguy.com, https://www.heliguy.com/blog/2018/12/12/drones-a-game-changer-say-police/ [Accessed 16 March 2021].

108 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en agosto de 2020, https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 [Accessed 16 March 2021].

109 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en agosto de 2020, https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 y Anderson, T. 2020, 'Avon and Somerset Constabulary's use of drones almost doubled over lockdown', ***The Canary*** https://www.thecanary.co/investigation/2020/11/25/avon-and-somerset-constabularys-use-of-drones-almost-doubled-over-lockdown/ [Accessed 16 March 2021].

110 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en agosto de 2020, https://www.whatdotheyknow.com/request/676650/response/1671179/attach/4/Response%20639%2020.pdf

111 Leprince-Ringuet, D. 2020, 'Police drones are taking to the skies', ***ZDNet,*** https://www.zdnet.com/article/police-drones-are-taking-to-the-skies/ [Accessed 16 March 2021].

112 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

113 BBC News, 2020, 'Manchester city-centre rave condemned by police', ***BBC News*** https://www.bbc.com/news/uk-england-manchester-55459614 [Accessed 16 March 2021].

Muchos de los drones que se utilizan en el Reino Unido son suministrados por la empresa china DJI[114]. El Mavic 2 Enterprise uno de los modelos típicos de drones que utiliza actualmente la policía británica. Al parecer, ***"cuesta unas 2.800 libras esterlinas, pesa menos de un kilo y tiene una autonomía de 29 minutos con un alcance de 5 km"***, según un artículo de Eleanor Langford en Politics Home[115].

El Servicio Aéreo de la Policía Nacional del Reino Unido (NPAS) está estudiando la posibilidad de comprar drones Hermes 900 mucho más grandes a la empresa israelí Elbit Systems[116], a pesar de que el dron Hermes ha sido desarrollado y probado en un contexto de guerra contra el pueblo palestino[117]. El dron israelí Hermes 900 ***"tiene una envergadura de 15 metros, pesa 970 kg y puede volar hasta 36 horas a 30.000 pies de altura"***[118]. Una de las justificaciones dadas por la NPAS para considerar estos drones es su potencial en la vigilancia de manifestaciones[119].

^ **Drone** Parrot **Anafi**, usado por la policía de Gales del Sur. Fuente: Wikimedia Commons/Dottensm Creative Commons License: BY-SA 4.0

> **Drone Hermes** de la empresa Elbit Systems. Fuente: Wikipedia Commons

114 Ver: Cleveland Police Drone Unit's Twitter. February 2020 https://twitter.com/DronesPolice/status/1227877097768726528, (Matrice is a DJI model), also FOI request made by Tom Anderson to South Wales Police in October 2020, https://www.whatdotheyknow.com/request/676650/response/1671179/attach/4/Response%20639%2020.pdf, and Kent Police website, Undated, 'Unmanned Aerial Vehicles', https://www.kent.police.uk/foi-ai/kent-police/who-we-are/who-we-are-and-what-we-do/unmanned-aerial-vehicle-drones/, [All accessed 16 March 2021].

115 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

116 Lewis, S, 2020, 'National Police Air Service tests potential of drone technology', Commercial Drone Professional, https://www.commercialdroneprofessional.com/national-police-air-service-tests-potential-of-drone-technology/ [Accessed 16 March 2021] and Asa Winstanley, 2020, 'British police may deploy Israeli drone used to kill Palestinians'***, The Electronic Intifada,*** https://electronicintifada.net/blogs/asa-winstanley/british-police-may-deploy-israeli-drone-used-kill-palestinians [Accessed 16 March 2021].

117 Stop the Wall, 2015, Supporting Israeli apartheid: EU funding for Elbit Systems, ***Stopthewall.org,*** Page 9 https://www.stopthewall.org/sites/default/files/horizon2020%20elbit.pdf [Accessed 16 March 2021], and Drone Wars UK, 2010, 'Israel and the Drone Wars', Page 7. https://dronewarsuk.files.wordpress.com/2014/01/israel-and-the-drone-wars.pdf [Accessed 16 March 2021].

118 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

119 *Ibid.*

Vigilancia de Estado: El caso de Reino Unido

3 EL ESTADO Y LAS EMPRESAS: DOS CARAS DE LA MISMA MONEDA

El aumento masivo del uso de la vigilancia de alta tecnología por parte de las fuerzas policiales y los organismos estatales está siendo defendido y promovido por dos actores principales. El primero es el propio Estado, ávido de medios cada vez más eficaces para vigilar y controlar a la población. El segundo son las empresas privadas, que obtienen enormes beneficios de la comercialización de la nueva tecnología. Estos dos actores se apoyan mutuamente. Las distintas ramas del Estado en el Reino Unido se aseguran de que las empresas se beneficien de las nuevas licitaciones de tecnología de vigilancia, mientras que a su vez el gobierno británico recibe presiones de las compañías privadas para que relaje las restricciones legales sobre el uso de la nueva tecnología. Al mismo tiempo, los detalles del uso de la tecnología de vigilancia por parte de la policía suelen mantenerse en secreto para el público, alegando consideraciones de seguridad nacional.

Este capítulo examina la estrecha relación entre las empresas y el gobierno del Reino Unido, y la actual falta de restricciones en el uso de la tecnología de reconocimiento facial, entre otros aspectos de la vigilancia de alta tecnología.

LA "PUERTA GIRATORIA"

No es de extrañar que los intereses del Estado y de las empresas privadas coincidan en lo que respecta a la tecnología de vigilancia. Existe una "puerta giratoria" entre las oficinas de las empresas que producen "alta tecnología" de vigilancia y Westminster. Por ejemplo, la Campaña contra el Comercio de Armas ha demostrado que, entre 2007 y 2020, al menos 31 personas pasaron de trabajar en BAE Systems a ocupar puestos en el gobierno o la administración pública, o viceversa. Además, la empresa recibió más de mil horas de tiempo del gobierno en forma de reuniones entre la empresa y los departamentos gubernamentales[120]. Esta estrecha relación ha generado claramente beneficios para BAE, que, por ejemplo, recientemente firmó un contrato multimillonario por el sistema de reconocimiento automático de matrículas a nivel nacional[121].

120 Campaign Against the Arms Trade, Undated, 'Influence,' Caat.org.uk, https://caat.org.uk/data/influence/org/3/meetings, [Accessed 16 March 2021].

121 Véase Capítulo 2.

El gobierno británico también está interesado en promover el éxito de las empresas de vigilancia del Reino Unido en el extranjero. Por ejemplo, la empresa británica FaceWatch ha exportado tecnología de reconocimiento facial del Reino Unido a Brasil, y se ha beneficiado del apoyo del Departamento de Comercio Internacional[122].

A raíz de la pandemia del Covid-19, el gobierno del Reino Unido llegó a acuerdos con empresas privadas que implicaban la puesta a disposición de estas empresas de cantidades masivas de datos de pacientes del Servicio Nacional de Salud (NHS). Se supone que estos datos permanecen bajo el control del NHS, pero los acuerdos han sido criticados por no tener en cuenta los problemas de privacidad. Una petición pública de Open Democracy argumentaba: ***"El almacén de datos COVID-19 contendrá información privada y personal de cada uno de los que dependemos del NHS. No queremos que nuestros datos personales caigan en manos equivocadas"***[123]. Una de las empresas que recibió un contrato fue Faculty, una compañía especializada en inteligencia artificial. Faculty está vinculada a Dominic Cummings, que en ese momento era el asesor jefe del Primer Ministro Boris Johnson. Faculty recibió 1,1 millones de libras por sus servicios al NHS[124].

122 Solicitud FOI realizada por Jo Griffin al Departamento de Comercio Internacional en 2019, https://www.whatdotheyknow.com/request/626720/response/1499993/attach/html/3/Final%20response%2005672.pdf.html [Accessed 16 March 2021].

123 Open Democracy, 2020, 'Stop the secrecy: Publish the NHS COVID data deals', https://www.opendemocracy.net/en/stop-secrecy-publish-nhs-covid-data-deals/ [Accessed 16 March 2021].

124 Open Democracy, 2020. 'Under pressure, UK government releases NHS COVID data deals with big tech', https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/?s=09&fbclid=IwAR23ZvPYNzrjlbktmXasn4jLt8O96999e4-tMDhofUqX9Vsf_68R94DiedA, [Accessed 16 March 2021].

PRESIONANDO PARA UNA VIGILANCIA SIN RESTRICCIONES

Las empresas privadas aprovechan su acceso ilimitado a los responsables de la toma de decisiones del gobierno para presionar (como lobby) contra las restricciones en el uso de la tecnología de vigilancia. Por ejemplo, las empresas que se dedican a la fabricación de drones están presionando a la Autoridad de Aviación Civil del Reino Unido para que levante las restricciones al vuelo de grandes aviones sin piloto[125]. Igualmente, BAE Systems y su socio estadounidense General Atomics pretenden que su dron "Protector" pueda volar en el espacio aéreo civil[126]. A su vez, el Ministerio de Defensa (MOD) se hace eco de estas peticiones, presionando también para que se modifique la normativa sobre el espacio aéreo para permitir las pruebas del dron. En última instancia, el Ministerio de Defensa quiere que el Protector se despliegue ***"en todo el espectro de operaciones"***, lo que incluye: fines de seguridad nacional, como la vigilancia; la formación del personal; y estar a disposición de las autoridades civiles para contingencias y emergencias[127].

RECONOCIMIENTO FACIAL: UNA TECNOLOGÍA NO REGULADA

En la actualidad, no existen limitaciones legales al uso de la tecnología de reconocimiento facial (FRT – Facial Recognition Technology) en el Reino Unido[128], aunque el Comisario de Información británico afirma que las imágenes captadas deben estar sujetas a la misma normativa de protección de datos que todo tipo de imágenes, y deben considerarse "datos sensibles"[129].

En 2019, un grupo multipartidista de diputados de Westminster firmó una carta en la que se pedía que se detuviera inmediatamente el uso de la FRT hasta que se estableciera una normativa[130]. Un proyecto de ley sobre la tecnología de reconocimiento facial automatizado (moratoria y revisión) pasó la primera lectura en la Cámara de los Lores en 2019, pero no ha avanzado más[131].

125 Drone Wars UK, 2019, 'General Atomics bring in BAE Systems to lobby for 'Protector' drone to fly in UK' https://dronewars.net/2019/01/28/general-atomics-bring-in-bae-systems-to-lobby-for-protector-drone-to-fly-in-uk/#more-11122 [Accessed 16 March 2021].

126 Drone Wars UK, 2019, 'General Atomics bring in BAE Systems to lobby for 'Protector' drone to fly in UK.'

127 Drone Wars UK, 2019, 'Take Action: Military drone use within UK', https://dronewars.net/military-drones-in-uk/ [Accessed 16 March 2021].

128 Big Brother Watch, Undated, 'Stop Facial Recognition', https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ [Accessed 16 March 2021].

129 Information Commissioner's Office, 2019, 'The use of live facial recognition technology by law enforcement in public places' https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion20191031.pdf [Accessed 16 March 2021].

130 Dearden, L. 2019, 'Police may have used 'dangerous' facial recognition unlawfully in UK, watchdog says', ***The Independent,*** https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-london-law-information-commissioner-latest-a9180101.html [Accessed 16 March 2021].

131 UK Parliament, 2019, 'Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] - Parliamentary Bills', ***Services. parliament.uk,*** https://services.parliament.uk/bills/2019-19/automatedfacialrecognitiontechnologymoratoriumandreview.html [Accessed 16 March 2021].

El Parlamento escocés ha pedido a la policía de Escocia que no utilice el FRT hasta que no haya demostrado una base legal para su uso[132]. En 2020, el Subcomité de Justicia del Parlamento escocés sobre la actuación policial publicó un informe en el que se afirmaba que no había base legal para los planes de la Policía de Escocia de empezar a utilizar esta tecnología. Police Scotland ha acordado no comprar la tecnología LFR, al menos por el momento[133].

Las empresas están aprovechando el vacío existente en cuanto a la regulación de las FRT y están aprovechando la oportunidad para comercializar sus productos a las autoridades del Reino Unido. Por ejemplo, FaceWatch comercializa su tecnología de reconocimiento facial a la policía y las autoridades locales del Reino Unido. En 2018, agentes de la Policía de Essex tuitearon sobre la asistencia a una prueba de FRT organizada por FaceWatch, a la que también asistió personal del Ayuntamiento de Southend[134].

En 2019, el Ayuntamiento de Waltham Forest, en Londres, llevó a cabo una prueba de tres días de reconocimiento facial en vivo (LFR). La tecnología para la prueba fue proporcionada gratuitamente por la empresa israelí AnyVision. Al proporcionar la prueba de forma gratuita, AnyVision estaba claramente tratando de poner un pie en la puerta para acceder al lucrativo mercado de contratación pública local del Reino Unido[135].

LA POLICÍA BRITÁNICA SIGUE ADELANTE CON LA LFR A PESAR DE LA SENTENCIA JUDICIAL

Ed Bridges es un ciudadano cuyo rostro fue captado con LFR por la policía de Gales del Sur mientras asistía a una protesta en Cardiff, y en otra ocasión cuando estaba de compras. Presentó una demanda contra la Policía de Gales del Sur, alegando que el uso de la tecnología había violado su derecho a la intimidad[136]. En un principio, el tribunal falló a favor de la policía, pero en agosto de 2020, el Sr. Bridges ganó su caso en una apelación presentada ante el Tribunal Superior. La organización Liberty, que representó a Bridges, declaró que la sentencia del Tribunal Superior significa que el uso de LFR por parte de la Policía de Gales del Sur debe detenerse[137].

132 Thomas, E. 2020. 'Facial recognition is in London. So how should we regulate it?' ***Wired UK,*** https://www.wired.co.uk/article/regulate-facial-recognition-laws [Accessed 16 March 2021].

133 Lynch, E. 2020. 'The Use of Live Facial Recognition Technology in Scotland: A New North-South Divide?' - ***UK Human Rights Blog,*** https://ukhumanrightsblog.com/2020/02/25/the-use-of-live-facial-recognition-technology-in-scotland-a-new-north-south-divide/ [Accessed 16 March 2021].

134 FOI request made by Pippa King to Southend on Sea Borough Council in July 2018, https://www.whatdotheyknow.com/request/facial_recognition_demonstration?unfold=1#incoming-1186570 [Accessed 16 March 2021].

135 Barnes, S. 2019, 'London council used facial recognition technology on streets without consulting residents'. ***The Telegraph,*** https://www.telegraph.co.uk/news/2019/10/07/london-council-used-facial-recognition-technology-streets-without/ [Accessed 16 March 2021].

136 The Times, 2019, 'Ed Bridges's challenge against facial recognition technology heads to Court of Appeal', https://www.thetimes.co.uk/article/ed-bridgess-challenge-against-facial-recognition-technology-heads-to-court-of-appeal-skjgdbhgd [Accessed 16 March 2021].

137 *Ibid.*

Bridges dijo después de la audiencia: ***"Esta tecnología es una herramienta de vigilancia masiva intrusiva y discriminatoria. La policía de Gales del Sur lleva tres años utilizándola contra cientos de miles de personas, sin nuestro consentimiento y a menudo sin nuestro conocimiento. Todos deberíamos poder utilizar nuestros espacios públicos sin ser sometidos a una vigilancia opresiva"***[138].

La abogada de Liberty, Megan Goulding, dijo: ***"El Tribunal ha acordado que esta distópica herramienta de vigilancia viola nuestros derechos y amenaza nuestras libertades... Es hora de que el Gobierno reconozca los graves peligros de esta tecnología intrusiva. El reconocimiento facial es una amenaza para nuestra libertad y debe prohibirse"***[139].

Sin embargo, en respuesta a la sentencia del Tribunal Superior, la Policía Metropolitana emitió un comunicado en el que afirmaba que su política en materia de LFR es *"diferente"* a la de la Policía de Gales del Sur, y dejaba claro que seguiría utilizándola[140]. La Policía de Gales del Sur también dijo que revisará su política a la luz de la sentencia, pero que seguirá desarrollando el uso de la tecnología[141].

En 2021, el informe de la Inspección de la Policía de Su Majestad (HMIC) respondió además al caso de Bridges. El informe analiza la sentencia del Tribunal Superior y concluye:

> ***"En definitiva, creemos que esta tecnología tiene un papel que desempeñar en muchas facetas de la labor policial, incluida la lucha contra los manifestantes que se comportan de ilegalmente de forma persistente. Esperamos que más fuerzas empiecen a utilizar el reconocimiento facial a medida que se desarrolle la tecnología"***[142].

A pesar de la sentencia del Tribunal Superior y de las preocupaciones públicas y parlamentarias sobre el LFR, el HMIC hizo de *"apoyar a las fuerzas para que utilicen la tecnología de reconocimiento facial en vivo"* una de sus recomendaciones clave en su informe de marzo de 2021 sobre la protesta policial[143].

138 *Ibid.*

139 *Ibid.*

140 Metropolitan Police UK, Undated, 'Update on facial recognition', Met.police.uk, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/ [Accessed 16 March 2021].

141 South Wales Police, Undated, 'What is AFR?', Afr.south-wales.police.uk.

142 HMIC, 'Getting the balance right', ***2021,*** page 45.

143 Ibid, page 5.

LA CULTURA DE SECRETISMO DE LA POLICÍA BRITÁNICA CON RESPECTO A LA TECNOLOGÍA DE VIGILANCIA

Durante la investigación de este informe, Shoal Collective realizó solicitudes de libertad de información (FOI) a las fuerzas policiales de todo el Reino Unido. Nos encontramos con una cultura de secretismo en lo que respecta al uso de la tecnología de vigilancia. El estricto control de la información disponible para el público sobre la vigilancia contrasta fuertemente con el acceso sin restricciones al gobierno, del que gozan las empresas que comercializan la tecnología.

> Drones:

Aunque la policía ha facilitado alguna información sobre el uso manifiesto de la tecnología de los drones, ninguno de los cuerpos policiales con los que nos pusimos en contacto reveló información sobre su uso encubierto, alegando cuestiones de seguridad nacional[144].

La Policía Metropolitana de Londres se negó a divulgar la información que solicitamos en virtud de la FOI, alegando que: "revelar las fechas [en las que el cuerpo] utilizó drones de forma manifiesta durante 2019-2020, ya sea de forma operativa o en pruebas, identificaría operaciones específicas y podría socavar nuestras funciones policiales"[145].

También preguntamos a la Policía Metropolitana en el marco de la FOI si la tecnología de los drones, o los drones que utilizan imágenes térmicas, se habían utilizado en la vigilancia de las protestas de Black Lives Matter (BLM) en Londres en 2020. La Policía Metropolitana de Londres dijo que no había utilizado estas tecnologías abiertamente, pero citó la amenaza del terrorismo como una razón para negarse a revelar si los drones se habían utilizado encubiertamente para este propósito. La respuesta dice así: ***"Aunque no se cuestionan los motivos del solicitante, confirmar o negar que se tiene cualquier otra información sobre el uso de cualquier equipo especializado con fines encubiertos, mostraría a los delincuentes cuál es la capacidad, las habilidades tácticas y las capacidades de la fuerza, permitiéndoles apuntar a áreas específicas del Reino Unido para llevar a cabo sus actividades criminales/terroristas. Confirmar o negar las circunstancias específicas en las que el servicio policial puede o no desplegar tales tecnologías conduciría a un aumento del daño a las investigaciones encubiertas y comprometería la aplicación de la ley"***[146].

144 Por ejemplo, véase la solicitud FOI realizada por Tom Anderson a la Policía de Kent en agosto de 2020, https://www.whatdotheyknow.com/request/676655/response/1616941/attach/html/3/20%2007%200870%20Response%20Letter.pdf.html y la solicitud FOI realizada por Tom Anderson a la Policía de Kent en septiembre de 2020, https://www.whatdotheyknow.com/request/676655/response/1633213/attach/html/4/20%2007%20870%20IR%20Response%20Letter.pdf.html [All accessed 16 March 2021].

145 Solicitud FOI realizada por Tom Anderson a la Policía Metropolitana en septiembre de 2020, https://www.whatdotheyknow.com/request/use_of_drones_by_the_met#incoming-1631947 [Accessed 16 March 2021].

146 Solicitud FOI realizada por Tom Anderson a la Policía Metropolitana en octubre de 2020, https://www.whatdotheyknow.com/request/surveillance_at_blm_protests#incoming-1667206 [Accessed 16 March 2021].

La Policía de Avon y Somerset se negó a facilitar el nombre de la empresa que fabrica sus drones, alegando que: "revelar información que permitiera identificar los vehículos aéreos no tripulados de la fuerza podría comprometer su finalidad operativa y permitir que fueran blanco de ataques"[147]. Del mismo modo, la Policía de Gales del Sur se negó a dar información sobre la frecuencia con la que utilizaban drones de forma encubierta, o cuáles utilizaban. Por último, preguntamos a la policía de Thames Valley en el marco de la FOI si se había utilizado la tecnología de los drones contra los activistas por el medio ambiente que han estado viviendo en casas en los árboles para protestar contra el ferrocarril de alta velocidad HS2. Una vez más, recibimos la respuesta de que la policía no podía "confirmar ni negar" si se habían utilizado drones[148].

> Tecnología de reconocimiento facial (FRT):

Presentamos solicitudes de FOI a la policía, buscando información sobre el uso de FRT y también recibimos respuestas similares. Solicitamos a la Policía Metropolitana que nos dijera en el marco de la FOI si se habían utilizado las FRT en la vigilancia de las protestas de BLM en Londres en 2020. La Policía Metropolitana de Londres respondió que no había utilizado estas tecnologías abiertamente, pero se negó a decir si se habían utilizado de forma encubierta, citando la amenaza de ***"actividades terroristas"***[149]. Del mismo modo, la Policía de Avon y Somerset se negó a responder si la fuerza utilizó el reconocimiento facial automático en sus operaciones encubiertas, o si la FRT se había utilizado de forma encubierta en la vigilancia de las protestas de BLM en Bristol en 2020[150]. La Policía de Thames Valley y la Policía de Kent también se negaron a responder a nuestras preguntas sobre el FRT[151].

147 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en agosto de 2020, https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 , [Accessed 16 March 2021].

148 Solicitud FOI realizada por Eliza Egret a la Policía de Thames Valley en noviembre de 2020, https://www.whatdotheyknow.com/request/696654/response/1669501/attach/3/3924%2020%20TVP%20Final%20Response%20Letter.pdf?cookie_passthrough=1, [Accessed 16 March 2021].

149 Solicitud FOI realizada por Tom Anderson a la Policía Metropolitana en septiembre de 2020, https://www.whatdotheyknow.com/request/use_of_drones_by_the_met#incoming-1631947 [Accessed 16 March 2021].

150 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en julio de 2020, https://www.whatdotheyknow.com/request/use_of_facial_recognition_techno_2#followup and August 2020, https://www.whatdotheyknow.com/request/blm_protests_2021#incoming-1644735 [Both accessed 16 March 2021].

151 Solicitud FOI realizada por Tom Anderson a la Policía de Avon & Somerset en julio de 2020, https://www.whatdotheyknow.com/request/696654/response/1669501/attach/3/3924%2020%20TVP%20Final%20Response%20Letter.pdf?cookie_passthrough=1 [Accessed 16 March 2021]

> IMSI Catchers:

Cuando los activistas intentan impugnar la negativa de la policía a revelar información sobre el estado de vigilancia del Reino Unido, los mecanismos de apelación disponibles suelen ser insuficientes. Por ejemplo, Privacy International ha trabajado incansablemente para tratar de obligar a la policía británica a ser más transparente sobre su uso de los IMSI-catchers, presentando varios recursos ante el Tribunal de Derechos de la Información. Lamentablemente, el tribunal confirmó la política de la policía de ***"ni confirmar ni negar"***[152].

Por lo tanto, no es de extrañar que en noviembre de 2020 la Policía Metropolitana nos dijera que ***"no confirmaría ni negaría"*** si los IMSI-catchers se habían utilizado en las protestas de Black Lives Matter a lo largo de ese año[153].

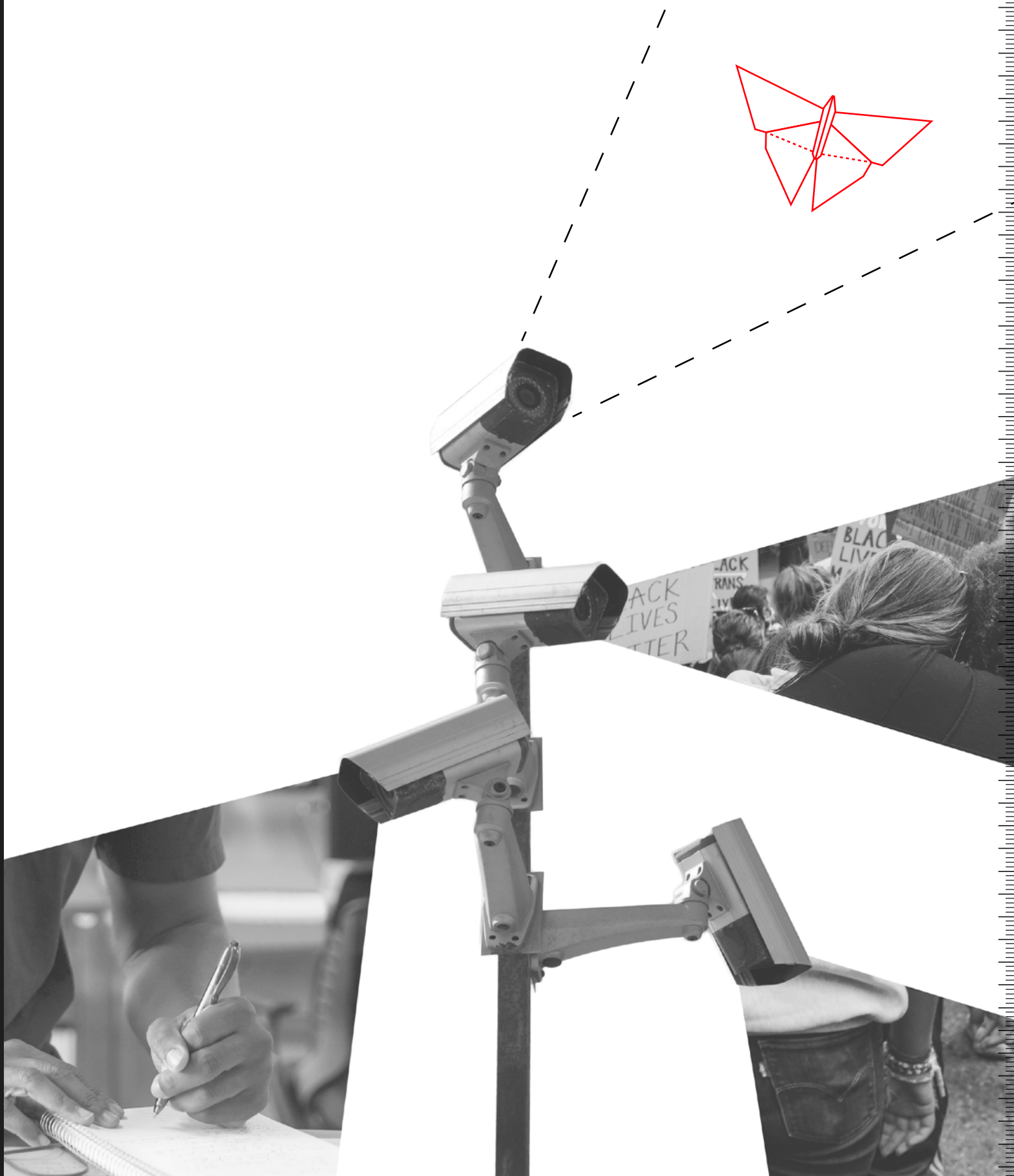
Protesta de Black Lives Matter protesters Oxford Street, Londres Fuente: Alisdare Hickson Flickr

152 Privacy International, 2019, 'Information Tribunal Decisions re IMSI Catchers: A loss for transparency and why we will continue the fight through other means', https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will [Accessed 16 March] 2021].

153 Solicitud FOI realizada por Eliza Egret a la Policía Metropolitana en noviembre de 2020, https://www.whatdotheyknow.com/request/imsi_catcher_use_on_blm_protests?nocache-incoming-1682649#incoming-1682649

Vigilancia de Estado: El caso de Reino Unido

4 EL EFECTO INTIMIDATORIO: VIGILANCIA Y SOCIEDAD CIVIL



El crecimiento exponencial de la vigilancia de alta tecnología en el Reino Unido ha tenido un efecto intimidatorio en los movimientos de base que luchan por el cambio social. Como ya hemos comentado, los movimientos sociales del Reino Unido han sufrido históricamente la represión, vigilancia policial y criminalización. Muchos de estos movimientos han sido objeto de campañas orquestadas por el Estado para deslegitimar a sus partidarios etiquetándolos como terroristas o extremistas domésticos, al margen de cualquier prueba que apoye esas afirmaciones[154]. La proliferación de nuevas tecnologías a disposición del Estado ha abierto nuevas vías para la represión a gran escala, en las que comunidades, poblaciones o movimientos enteros pueden ser vigilados sin que se den cuenta de que son el objetivo. Como se demostrará más adelante, sus efectos negativos suelen afectar más a las comunidades de la clase trabajadora y a las personas racializadas. En este capítulo daremos algunos ejemplos del efecto de estas nuevas tecnologías sobre la disidencia en el Reino Unido, prestando especial atención a la dimensión clasista y racial del uso de esta tecnología.

LOS PODERES DE LA POLICÍA UTILIZADOS PARA LLEVAR A CABO "CACHEOS DIGITALES"

En el Reino Unido, la policía está facultada para incautar dispositivos electrónicos cuando las personas están bajo arresto, durante las redadas en los domicilios y cuando las personas son detenidas en virtud del Anexo 7 de la Ley de Terrorismo en las fronteras del Reino Unido[155]. Alastair Lyon, de la firma de abogados Birnberg Peirce, cree que el Anexo 7 se utiliza a menudo para llevar a cabo un "registro digital" de los activistas. Lyon dijo a Shoal Collective:

> *"La definición de terrorismo es lo suficientemente amplia como para que enormes áreas de actividad política legítima puedan entrar en ella. Las respuestas de las entrevistas del Anexo 7 no suelen poder utilizarse en los tribunales. El proceso de hacer preguntas no parece ser el objetivo de la mayoría de las paradas: las respuestas dadas en las propias entrevistas son probablemente las que menos interesan a la policía. El "cacheo digital" parece ser el objetivo. Los dispositivos digitales confiscados pueden retenerse durante un máximo de siete días, a menos que se retengan después para una investigación penal. Los dispositivos dan a la policía acceso a gran parte de tu vida y tus relaciones. Esto es clave: la policía está creando potencialmente una enorme base de datos con esta información"*[156].

154 Véase Capítulo 1.

155 Network for Police Monitoring, 2012, 'Schedule 7 terror laws used to interrogate activists', https://netpol.org/2012/12/12/schedule-7-terror-laws-used-to-interrogate-activists/ [Accessed 16. March 2020].

156 Entrevista realizada por Shoal Collective a Alastair Lyon, de Birnberg Peirce solicitors, 2020.

Una vez que la policía ha incautado los dispositivos, puede utilizar los servicios de extracción de datos proporcionados por empresas como Cellebrite[157] para controlar los datos personales de la población. Estos "cacheos digitales" se han convertido en una herramienta importante en la represión de los participantes de los movimientos sociales.

LA VIGILANCIA POLICIAL DE LAS COMUNICACIONES TIENE UN "EFECTO INTIMIDATORIO EN LAS PROTESTAS"

Las nuevas tecnologías, como los IMSI-catchers, tienen un impacto significativo en el derecho a la privacidad, al adquirir de forma encubierta datos personales a través de los teléfonos móviles, lo que hace casi imposible ser anónimo en una multitud[158]. Los datos extraidos pueden utilizarse para vigilar las actividades de una persona y crear un perfil. Shoal Collective habló con Llia Siatitsa, Directora de Programas de Privacy International, quien explicó la forma en la que tecnologías como los IMSI-catchers afectan a la capacidad de organización de las personas:

> *"Las nuevas tecnologías de vigilancia están transformando radicalmente la capacidad de las autoridades para controlar las protestas. Ya son capaces de llevar a cabo una vigilancia generalizada, invisible y en tiempo real de las protestas, a distancia, sin que la gente lo sepa o lo consienta, mediante el uso de nuevas tecnologías, como los IMSI-catchers. Planificar y participar en las protestas requiere que nos comuniquemos libremente y de forma confidencial sin interferencias ilegales. Hasta ahora, la mayoría de estas tecnologías de vigilancia se han desplegado sin transparencia ni un marco legal y de supervisión adecuado. El uso de estas tecnologías intrusivas es una injerencia grave e injustificada en nuestra intimidad, pero también puede vulnerar directamente nuestra libertad de reunión y tener un efecto intimidatorio en las protestas, ya que disuade a la gente de participar en ellas"*[159].

157 Véase Capítulo 2.

158 Véase Capítulo 2.

159 Esta cita fue obtenida por Shoal Collective como parte de la investigación para este informe, y el relato y las opiniones expresadas son únicamente las del entrevistado.

EL RECONOCIMIENTO FACIAL EN VIVO Y LA AMENAZA A LA DISIDENCIA

Daragh Murray, coautor de un informe de la Universidad de Essex de 2019 sobre el reconocimiento facial en vivo, explica el potencial represivo de su uso:

> *"El reconocimiento facial en vivo (LFR) interfiere con el derecho a la vida privada, pero el impacto de esta tecnología va mucho más allá de este derecho. La tecnología LFR identifica a una persona en tiempo real mediante el procesamiento biométrico. La combinación de LFR con otras fuentes de datos puede revelar mucho sobre la vida profesional y privada de una persona... Los perfiles individuales detallados que permite el reconocimiento facial avanzado pueden utilizarse para fundamentar diversas decisiones relacionadas, por ejemplo, con los derechos al trabajo, a la salud o a la asistencia social. ¿Qué significará para la forma en que las personas se relacionan con quienes las rodean, si todas sus actividades se registran y se utilizan para informar sobre decisiones que pueden cambiar su vida? Una preocupación real es que la gente tenga miedo de participar en los márgenes de la sociedad, y que modifique su comportamiento hacia la corriente principal"*[160].

Tecnología de reconocimiento facial siendo utilizada para controlar a manifestantes en Gales del Sur. Fuente: Emily Apple de "Network for Police Monitoring" (con permisos)

160 University of Essex, 2019, 'Live facial recognition: the impact on human rights and participatory democracy', https://www.essex.ac.uk/blog/posts/2019/11/07/live-facial-recognition-the-impact-on-human-rights-and-participatory-democracy [Accessed 16 March 2021].

En este capítulo daremos algunos ejemplos del efecto de estas nuevas tecnologías sobre la disidencia en el Reino Unido. Está claro que una de las funciones de la LFR para la Policía Metropolitana de Londres y la Policía del Sur de Gales es el control de la disidencia política. Por ejemplo, la policía de Gales utilizó la LFR en una operación de seguridad para una visita real en 2018. Este tipo de visitas han sido previamente objeto de controversia política y protestas[161]. En marzo de 2018, la Policía del Sur de Gales desplegó un furgón policial equipado con cámaras LFR para controlar una protesta antimilitarista frente a la exposición de armas Defence Procurement, Research, Technology & Exportability (DPRTE) en el Motorpoint Arena de Cardiff[162].

- En 2020, la policía metropolitana optó por llevar a cabo una prueba de reconocimiento facial en Oxford Circus, una zona a menudo frecuentada en protestas políticas[163].
- En 2017, la Policía Metropolitana utilizó el LFR para vigilar la ceremonia anual del Día del Recuerdo. El cuerpo admitió que personas que no eran buscadas para ser arrestadas estaban en una "lista de vigilancia" de LFR, porque la policía sospechaba que podrían perturbar el "plan de seguridad" del evento[164]. Esto demuestra que la policía no se va a contentar con utilizar la tecnología LFR para identificar a las personas buscadas, sino que va a ampliar sus redes en términos de vigilancia y recopilación de datos. Podrían utilizar el LFR para realizar detenciones preventivas y para acosar a quienes consideren que perturban sus actividades.

Estos ejemplos de utilización de la LFR para atacar las protestas políticas son muy preocupantes y podrían disuadir a la gente de participar en las manifestaciones. El uso de esta tecnología pone de manifiesto que cada vez es más difícil permanecer en el anonimato cuando se asiste a las protestas, y podría significar que los principales organizadores sean señalados por la tecnología y sometidos a acoso policial.

161 South Wales Police, April 2020, 'All Deployments', ***Afr.south-wales.police.uk,*** https://afr.south-wales.police.uk/wp-content/uploads/2020/04/All-Deployments.pdf [Accessed 16 March 2021].

162 Apple, E. 2018, 'South Wales Police under fire for using facial recognition technology against protesters', ***The Canary,*** https://www.thecanary.co/uk/2018/03/29/south-wales-police-under-fire-for-using-facial-recognition-technology-against-protesters/ [Accessed 16 March 2021].

163 FOI request made by Phil Booth to the Metropolitan Police in July 2020, https://www.whatdotheyknow.com/request/648561/response/1610448/attach/html/5/20%2003%2006%20LFR1%20URN%20 2020%20002%20BOOTH%20FOIA%20REDACTED%20WAD%20Q1.PDF.pdf.html [Accessed 16 March 2021].

164 FOI request by Big Brother Watch to the Metropolitan Police in March 2018, https://bigbrotherwatch.org.uk/wp-content/ uploads/2018/04/Metropolitan-Police-20180300000548.pdf [Accessed 16 March 2021].

LFR: UNA TECNOLOGÍA INEXACTA Y CON SESGO RACIAL

La tecnología de reconocimiento facial en vivo (LFR, en su acrónimo en inglés) también es extremadamente inexacta en lo que respecta a la identificación de determinados rostros, mostrando un sesgo racial y de género muy preocupante y que perpetúa la discriminación racial y de género existente, ya tan arraigada en la sociedad. El informe de la Universidad de Essex descubrió que: ***"En las seis pruebas que se evaluaron, la tecnología LFR hizo 42 coincidencias - en sólo ocho de esas coincidencias los autores del informe pueden decir con absoluta confianza que la tecnología acertó"***[165]. Big Brother Watch afirma que: ***"El reconocimiento facial de la policía metropolitana fue un 93% inexacto entre 2016 y 2019"*** y que ***"más de 3.000 personas [habían sido] identificadas erróneamente por el reconocimiento facial de la policía"***[166]. Un estudio realizado en 2018 por el Instituto Tecnológico de Massachusetts (MIT) demostró que la tecnología presentaba más errores en el caso de las mujeres y de las personas no blancas, ya que el conjunto de datos utilizado para probar la precisión del software era ***"un 77% de hombres y más de un 83% de personas blancas"***[167].

A pesar de las crecientes pruebas que demuestran que la tecnología de reconocimiento facial (FRT) es extremadamente inexacta a la hora de identificar los rostros de las personas, salvo los de los hombres blancos, la policía del Reino Unido no ha tomado hasta ahora medidas para eliminar la FRT de su kit de herramientas de vigilancia digital. Se sigue utilizando esta tecnología que tiene un sesgo racial y de género negativo contra las personas racializadas en particular, y las mujeres en general.

La BBC informó en 2019 de que un "antiguo jefe de reconocimiento facial" de la policía británica había señalado en 2014 "que la etnia puede tener un impacto en la precisión de las búsquedas [de reconocimiento facial]". Había pedido a CGI, la empresa canadiense que gestiona la base de datos de imágenes faciales de la policía, que investigara la cuestión. Sin embargo, la policía no parece haber dado seguimiento a estas preocupaciones[168].

El informe de 2021 del HMIC sobre la vigilancia de las protestas reconoce que la tecnología FRT tiene un sesgo racial, pero se limita a decir que la policía sigue trabajando para garantizar: ***"que se minimice el sesgo desproporcionado contra las comunidades negras, asiáticas y de minorías étnicas"***[169]. El informe no tiene ninguna respuesta a la pregunta de cómo la policía es capaz de asegurar eso.

165 Human Rights, Big Data & Technology Project, the University of Essex Human Rights Centre, 2019, 'HRBDT Researchers Launch New Report on London Metropolitan Police's Trial of Live Facial Recognition Technology' ***HRBDT,*** https://www.hrbdt.ac.uk/hrbdt-researchers-launch-new-report-on-london-metropolitan-polices-trial-of-live-facial-recognition-technology/ [Accessed 16 March 2021].

166 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk.

167 Massachusetts Institute of Technology, 2018, 'Study finds gender and skin-type bias in commercial artificial-intelligence systems', https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [Accessed 16 March 2021].

168 White, G. 2019, 'Use of facial recognition tech 'dangerously irresponsible'', https://www.bbc.co.uk/news/technology-48222017 [Accessed 16 March 2021].

169 ***HMIC,*** 'Getting the balance right', page 48.

El asesinato de Rashan Charles, que murió tras ser retenido por agentes de la Policía Metropolitana en 2017[170], y las muertes de tantas otras personas de color a manos de la policía británica[171] muestran lo profundamente racista que es la policía del Reino Unido como institución. Las personas de color tienen el doble de probabilidades de ser disparadas por la policía en el Reino Unido que las personas blancas[172], y una persona negra o de origen asiático tiene el doble de probabilidades de morir bajo custodia policial que una persona blanca si se recurre a la contención o al uso de la fuerza, o cuando la persona detenida registra problemas de salud mental[173]. Por lo tanto, es muy inquietante que una fuerza policial que ya tiene prejuicios raciales confíe en herramientas digitales que en sí mismas también tienen prejuicios raciales, con el fin de identificar a las personas de interés. Estas herramientas poco fiables sólo pueden exacerbar el sentimiento de desconfianza en la policía.

La Policía Metropolitana también ha utilizado la LFR de forma racializada y clasista. Según el censo de 2011, en Stratford, la zona de Londres donde la Policía Metropolitana desplegó la LFR en tres ocasiones[174], el 54% de los residentes no habían nacido en el Reino Unido[175] y más del 20% son musulmanes. El 52% de los niños del Borough de Newham, la parte de Londres en la que se encuentra Stratford, viven en la pobreza, en comparación con un total del 38% en todo Londres[176]. En 2016 y 2017, la Policía Metropolitana desplegó la tecnología LFR en el Carnaval de Notting Hill[177], un festival anual protagonizado por miembros de la comunidad antillana. El carnaval ha sido históricamente reprimido por la policía, y suele ser un punto álgido en el que la ira contra la policía racializada de Londres se extiende a las calles[178].

Las fuerzas policiales del Reino Unido ya practican una violencia racial sistemática. Si a esta mezcla se le añade un algoritmo inexacto y con sesgo racial, la combinación es preocupante.

170 Townsend, M. 2017, 'Police watchdog calls for Met officer in custody death inquiry to be suspended', ***The Guardian,*** https://www.theguardian.com/uk-news/2017/sep/16/police-met-ipcc-custody-death-rashan-charles [Accessed 16 March 2021].

171 Inquest, 2021, 'BAME deaths in police custody', https://www.inquest.org.uk/bame-deaths-in-police-custody [Accessed 16 March 2021].

172 Qasim, W. 2020, 'The UK is Not Innocent – Police Racism Has a Long and Violent History Here Too', ***Novara Media,*** https://novaramedia.com/2020/06/01/the-uk-is-not-innocent-police-brutality-has-a-long-and-violent-history-here/ [Accessed 16 March 2021].

173 Inquest, 2021, 'BAME deaths in police custody'.

174 Big Brother Watch, Undated, 'Stop Facial Recognition'.

175 'Stratford and New Town Demographics (Newham, England)', Stratford-and-new-town.localstats.co.uk,lable at: http://stratford-and-new-town.localstats.co.uk/census-demographics/england/london/newham/stratford-and-new-town [Accessed 16 March 2021]. and Statistics, 2018, 'Population of England and Wales'. ***Ethnicity-facts-figures.service.gov.uk***, https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/national-and-regional-populations/population-of-england-and-wales/latest [Accessed 16 March 2021].

176 Trust for London, Undated, 'Poverty and Inequality Data For Newham', https://www.trustforlondon.org.uk/data/boroughs/newham-poverty-and-inequality-indicators/ [Accessed 16 March 2021].

177 Brown, J. 2019, 'Police use of live facial recognition technology: Challenges and concerns', ***House of Commons Library,*** https://commonslibrary.parliament.uk/police-use-of-live-facial-recognition-technology-challenges-and-concerns/ [Accessed 16 March 2021].

178 White, J. 2020, 'Police, Press & Race in the Notting Hill Carnival 'Disturbances'' ***History Workshop,*** https://www.historyworkshop.org.uk/notting-hill-carnival-disturbances/ [Accessed 16 March 2021]. and Youle. E. 2020, 'Exclusive: New Data Reveals Crime Should Not Be The Story Of Notting Hill Carnival', HuffPost UK, : https://www.huffingtonpost.co.uk/entry/notting-hill-carnival-arrest-rates-same-as-glastonbury_uk_5d5d1d18e4b063487e9519d5?guccounter=2&guce_referrer=aHR0cHM6Lyg kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAH8ymTxlUXmo5xtMZyDvhNcIJUZtsqAKiEPtf7Gw7ZuSsuKwOJtPhOnWryFyIZbe2TVc-voUA8GAvaAv_sxfROLEO85wge-aaizxKjYTsU6JzndnK2uN_vG77hSAvV2BJrTumfDgpA02UkeRJcadhj8M7hZG9_0sP_1yrjWNKcS- [Accessed 16 March 2021].

HACKEAR LOS TELÉFONOS DE PERIODISTAS Y ORGANIZADORES DEL REINO UNIDO

La empresa israelí NSO Group es uno de los mayores fabricantes de malware del mundo. Vende la tecnología exclusivamente a los gobiernos[179]. Su software espía Pegasus se describe como "un programa tan sofisticado que puede incrustarse en tu teléfono móvil a través de una sola llamada telefónica, incluso si no coges esa llamada"[180]. En 2018, los investigadores de Citizen Lab "identificaron un total de 45 países en los que los operadores de Pegasus podrían estar llevando a cabo operaciones de vigilancia", incluido el Reino Unido[181]. Aunque la naturaleza de dicha tecnología hace difícil determinar si el gobierno del Reino Unido la utiliza para espiar a los ciudadanos británicos; en 2020, NSO apareció en la exposición anual de Seguridad y Policía del Ministerio del Interior[182] y está previsto que aparezca en la Exposición Internacional de Seguridad de 2021 en Londres[183].

Los residentes del Reino Unido también han sido objeto de incidentes de hackeo y vigilancia transfronterizos, que probablemente provienen de gobiernos extranjeros. NSO fue noticia en el Reino Unido en 2018 cuando se reveló que su software espía Pegasus había sido utilizado en un intento de hackear el teléfono de un empleado de la ONG británica Amnistía Internacional[184]. En este caso, un hacker utilizó WhatsApp para intentar instalar el malware. Si el empleado hubiera hecho clic en un enlace del mensaje de WhatsApp, su teléfono habría instalado Pegasus sin su conocimiento, y habría tenido acceso a todos los datos del teléfono[185].

Varios otros residentes en el Reino Unido han sido objeto del malware Pegasus, entre ellos el satírico saudí afincado en Londres Ghanem Almasarir, el activista político Yahya Assiri y Faustin Rukundo, miembro de un grupo de la oposición ruandesa que vive en el exilio[186].

Aunque los citados ciberataques transfronterizos no fueron llevados a cabo por el gobierno británico, muestran el peligroso potencial de tecnologías como Pegasus.

179 Amnesty International, 2018, 'Meet NSO Group: a go-to company for human rights abusers', ***Amnesty.org.uk***, https://www.amnesty.org.uk/meet-nso-group-go-company-human-rights-abusers [Accessed 16 March 2021].

180 Big Brother Watch, 2019,'Surveilling journalists from inside their phones', ***Bigbrotherwatch.org.uk***, https://bigbrotherwatch.org.uk/2019/12/surveilling-journalists-from-inside-their-phones/ [Accessed 16 March 2021].

181 Marczak, B. Scott-Railton, J. McKune, S. Razzak, B. and Deibert, R. 2018, 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries'. ***The Citizen Lab*** https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ [Accessed 16 March 2021].

182 Security and Policing, Undated, 'Exhibitors list 2020: NSO Group', Securityandpolicing. https://www.securityandpolicing.co.uk/exhibitors/exhibitors-list-2020/nso-group/ [accessed October 2020].

183 International Security Expo 2021, Undated, 'Exhibitors', ***Internationalsecurityexpo.com***, https://www.internationalsecurityexpo.com/exhibitors/nso-group?&azletter=N&searchgroup=libraryentry-exhibitors [Accessed 16 March 2021].

184 Amnesty International, 2018, 'Meet NSO Group: a go-to company for human rights abusers'.

185 Ibid. and Marczak, B. Scott-Railton, J. McKune, S. Razzak, B. and Deibert, R., 2018. ***HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.***

186 Brewster, T. 2018, 'Exclusive: Saudi Dissidents Hit With Stealth iPhone Spyware Before Khashoggi's Murder', ***Forbes,*** https://www.forbes.com/sites/thomasbrewster/2018/11/21/exclusive-saudi-dissidents-hit-with-stealth-iphone-spyware-before-khashoggis-murder/?sh=7018d2f22e8b a [Accessed 16 March 2021].and Hughes, S. Evans. R. Kirchgaessner, S. 2020. 'UK to host spyware firm accused of aiding human rights abuses', ***The Guardian,*** https://www.theguardian.com/world/2020/feb/06/uk-to-host-spyware-firm-accused-of-aiding-human-rights-abuses [Accessed 16 March 2021].

SISTEMA RAM PARA CONTROLAR A LOS PARTICIPANTES DE MOVIMIENTOS SOCIALES

En 2005, la policía detuvo al activista antimilitarista John Catt y a su hija Linda después de que su coche fuera señalado por la tecnología de Reconocimiento Automático de Matrículas (RAM). Había sido incluido en una "lista caliente" del RAM después de que la policía observara la matrícula del coche de Catt en una manifestación ante la fábrica de armas EDO MBM.

Según The Guardian:

> *"...la furgoneta había pasado por debajo de una cámara de reconocimiento automático de matrículas (RAM) en el este de Londres, lo que provocó una alerta: "De interés para la Unidad de Orden Público, policía de Sussex". En cuestión de segundos, Catt, de 50 años, y su padre, John, de 84, fueron detenidos por la policía y registrados en virtud de la Ley de Terrorismo"*[187].

Ni John ni Linda tenían antecedentes penales y no fueron detenidos ni acusados de ningún delito[188].

Varias otras personas que participan en movimientos de acción directa se han quejado de que la policía les ha dado el alto en repetidas ocasiones después de que su coche fuera señalado por la policía. Según The Guardian en 2009, se dijo a los agentes que podían ***"colocar "marcadores" contra los vehículos de cualquier persona que asista a manifestaciones utilizando el centro nacional de datos RAM en Hendon, al norte de Londres, que almacena información sobre los desplazamientos de los coches desde hace hasta cinco años"***[189].

Más recientemente, la amenaza del sistema RAM se ha utilizado para controlar los movimientos de la gente durante el cierre de Covid-19. En 2020, el gobierno galés amenazó con utilizar el reconocimiento automático de matrículas para rastrear los coches que cruzaran la frontera desde Inglaterra[190]. Aunque estas restricciones de viaje pueden parecer relativamente benignas en el contexto de la crisis sanitaria, el uso de esta tecnología como amenaza muestra el poder que tiene el Estado para controlar los movimientos de la población.

187 Lewis, P. Evans, R. 2009, 'Activists repeatedly stopped and searched as police officers 'mark' cars', ***The Guardian,*** https://www.theguardian.com/uk/2009/oct/25/surveillance-police-number-plate-recognition [Accessed 16 March 2021].

188 *Ibid.*

189 *Ibid.*

190 Sheridan. E. 2020. 'Welsh police could use ANPR to identify people travelling across border from England', ***The Telegraph,*** https://www.telegraph.co.uk/politics/2020/10/15/welsh-police-could-use-anpr-identify-people-travelling-across/ [Accessed 16 March 2021].

USO DE DRONES PARA ACOSAR A LOS MANIFESTANTES

Uno de los entrevistados, participante en el campamento de protesta Power Beyond Borders de 2019 en Hertfordshire que prefirió permanecer en el anonimato, recalcó los efectos del uso de la tecnología de los drones en un contexto de protesta:

> *"Participé en el campamento de acción masiva de Reclaim the Power a finales de julio de 2019. Fue en Hodderston Hertfordshire, justo al norte de Londres, y situado muy cerca de la central eléctrica de Rye House, propiedad de Drax... Fue en la última etapa del evento en el campamento de Hodderston cuando y donde presencié la vigilancia con drones.*
>
> *...en el momento en que vi los drones, era de día. Hablé con otras personas del campamento sobre los drones, y todos tenían una opinión similar. Todos pensamos que su uso era excesivamente intrusivo. Probablemente, su objetivo era, en parte, hacernos sentir incómodos y vigilados"*[191].

Las personas que entrevistamos también nos dijeron que -además del campamento Power Beyond Borders- se utilizaron drones para vigilar una protesta celebrada en 2020 en Bristol para conmemorar la muerte de una residente de la ciudad, Anna Campbell. Anna fue asesinada en el noreste de Siria (Rojava) mientras participaba en la resistencia armada contra la invasión turca. Los liberadores de animales también nos dijeron que la policía había utilizado drones para vigilar los intentos de sabotear el sacrificio de tejones en Devon[192]. Según el informe HMIC de 2021, se utilizaron drones para vigilar a los manifestantes de la Rebelión de la Extinción en el aeropuerto de Bristol en agosto de 2020[193].

191 Shoal Collective, entrevista con un participante del campamento Power Beyond Borders de 2019 realizada en agosto de 2020.

192 Shoal Collective, entrevistas con activistas, 2020.

193 *HMIC,* 'Getting the balance right', page 46.

ESTUDIO DE CASO

Los efectos de la vigilancia policial sobre un simpatizante internacionalista del Movimiento de Liberación del Kurdistán

Shoal Collective habló con Nik Matheou, internacionalista del Movimiento de Liberación del Kurdistán con sede en Londres. Describió cómo el movimiento experimenta constantemente la represión policial, y cómo la policía extrajo datos telefónicos en un intento de perseguir a su camarada, Josh Schoolar[194]:

> *"Desde finales de 2016, y durante todo el año 2017, Josh estuvo en Siria, en Rojava... Fue inicialmente a hacer un voluntariado civil... Seis meses después decidió unirse al Batallón Internacional de la Libertad, que es un batallón de las Unidades de Protección Popular (YPG), formado por grupos anarquistas y comunistas de Turquía y de todo el mundo. Luchó con ellos durante varios meses, participando en la liberación de Raqqa [del Daesh/ISIS]. Tras la liberación de Raqqa, se quedó un par de meses más y luego volvió a casa".*

El YPG no es un grupo terrorista ilegal en el Reino Unido. De hecho, un jurado británico en el caso de Aidan James -otro combatiente del YPG- determinó que no era un delito que James se uniera a la lucha del YPG contra Daesh[195].

Josh llevaba seis meses de vuelta de Siria cuando fue detenido por la policía en virtud del Anexo 7. Mattheou continuó:

> *"En noviembre de 2018, fuimos a Europa continental. Sin embargo, al volver, nos entrevistaron en el marco del Anexo 7 en la frontera de Dover. Ese fue el comienzo de la represión para Josh. Fue interrogado por separado en una sala diferente a la nuestra sobre su estancia en Siria... Le quitaron el teléfono... y se lo devolvieron dos o tres días después".*

Mattheou continuó describiendo cómo en julio de 2019 Josh fue detenido de nuevo:

> *"Acababa de volver a casa de un festival de Plan C [Plan C es una organización de izquierda antiautoritaria]. Fue detenido en su casa. Se registró su casa y se le quitó el teléfono y el portátil, y se lo llevaron para interrogarle...*

194 Este estudio de caso se basa en una entrevista realizada como parte de la investigación para este informe, y el relato y las opiniones expresadas son únicamente las del entrevistado.

195 Judiciary UK, 2019, 'Sentencing Remarks', Judiciary.uk, https://www.judiciary.uk/wp-content/uploads/2019/11/SENTENCING-REMARKS.pdf [Accessed 16 March 2021].

Su lugar de trabajo fue allanado, según tengo entendido, por policías armados. Josh era profesor de educación especial en una escuela de Manchester.

La policía de Manchester se llevó su teléfono, lo que significó que tuvieron otra oportunidad de intentar recuperar las cosas. Posteriormente, a través de la comunicación con su abogado, confirmaron que tenía imágenes en su teléfono que demostraban que había recibido entrenamiento con armas en Siria. Por lo tanto, el teléfono que se llevó fue la prueba clave que pretendían reunir. Es importante decir, sin embargo, que aunque continuó siendo investigado en virtud del Anexo 5 de la Ley de Terrorismo -preparación de actos de terrorismo- nunca fue acusado de nada [ya que el YPG no es un grupo ilegal].

La redada en su lugar de trabajo alertó a la escuela. En realidad, ya se les había informado de su estancia en Siria. Había obtenido pruebas de su buen comportamiento mientras estaba allí. No había constancia de que la Asayish, la policía del norte de Siria, hubiera tenido nunca ningún problema con él, y tenía la confirmación de que había estado enseñando inglés en Kobanê. Desgraciadamente, la escuela lo despidió, aunque no había sido acusado por la policía [del Reino Unido]".

Mattheou describió los efectos de esta represión en la vida de Schoolar:

"En términos de los efectos en la vida de Josh, fueron profundos. Realmente no puedo creer que el asalto a su escuela fuera otra cosa que un intento de hacer lo que consiguió: que lo despidieran y arruinaran su oportunidad de seguir la carrera como profesor que él había elegido. Tuvo que cambiar radicalmente su visión de lo que iba a hacer en su vida a partir de ese momento. También afectó a su vida porque en ese momento le quitaron el pasaporte.

Y le creó un problema general para poder sentirse seguro con la comunicación con los amigos cercanos. Si se comunicaba con sus amigos y luego se descubría a través de sus aparatos electrónicos, potencialmente supondría un caso más fuerte contra ellos. Por lo tanto, no lo hizo. Era un pánico constante de bajo nivel.

Perdió su forma de pagar el alquiler. Tuvo que mudarse de casa durante varios meses antes de poder volver a Manchester. Realmente redefinió todo los dos últimos años de su vida antes de que lamentablemente falleciera".

CONCLUSIONES

El Imperio Británico utilizó durante siglos técnicas de vigilancia, espionaje, recogida de datos y control para imponer su dominio a las poblaciones colonizadas y reprimir la disidencia. Sin embargo, los avances tecnológicos, junto con las narrativas de seguridad nacional del Estado en las últimas dos décadas, han permitido la creación de una sociedad de la vigilancia masiva.

La vigilancia estatal se utiliza junto con la violencia policial y la violencia del sistema penitenciario para controlar la disidencia. El estado de vigilancia, cada vez más extendido, tiene un efecto escalofriante sobre la participación en los movimientos sociales por el cambio, ya que permite la persecución, el acoso y la criminalización de los participantes de los movimientos sociales.

El crecimiento de la sociedad de la vigilancia en el Reino Unido está siendo impulsado por empresas privadas, deseosas de obtener beneficios de la creciente demanda de nuevas tecnologías, y por el gobierno británico, deseoso de controlar a la población. Estos actores tienen intereses que se solapan. Las empresas privadas presionan al gobierno (como lobby) para que reduzca la regulación de la tecnología de vigilancia, mientras que las instituciones estatales utilizan esa falta de regulación para ampliar la red de vigilancia.

El alcance total del uso de la tecnología de vigilancia por parte de la policía se mantiene en secreto para el público. Este velo de secretismo se mantiene gracias a las respuestas de la policía de ***"ni confirmar ni negar"*** a muchas solicitudes públicas.

La tecnología de vigilancia también se utiliza de forma injusta y discriminatoria contra la clase trabajadora y los colectivos racializados. En particular, las fuerzas policiales del Reino Unido se niegan a dejar de utilizar la tecnología de reconocimiento facial en vivo (LFR), a pesar de reconocer que tienen un sesgo racial.

La aplicación ***discriminatoria*** de la draconiana legislación antiterrorista del Reino Unido hace que determinadas comunidades sean tratadas con recelo y criminalizadas. Por ejemplo, los musulmanes, los tamiles y los kurdos se enfrentan a una vigilancia policial aún mayor en virtud de su religión o etnia.[196] El gobierno del Reino Unido también está impulsando nuevas leyes represivas de tránsito, que destruirán los medios de vida de las comunidades gitanas, romaníes y nómadas.[197] Este trato desigual de ciertas comunidades dentro del estado de vigilancia del Reino Unido es una continuación del legado colonial británico.

Las tecnologías intrusivas y represivas descritas en este informe dejan un poder cada vez mayor en manos de la policía y otras autoridades. Hasta ahora, este poder ha quedado en gran medida sin control. La experiencia de la vigilancia ma-

196 Véase Capítulo 1.

197 No Fixed Abode Travellers and Supporters, Undated, 'Campaigns'.

siva en el Reino Unido ilustra que la monitorización de nuestra vida cotidiana y la recopilación de nuestros datos personales seguirán utilizándose para controlar a la disidencia y silenciar las voces radicales.

Es necesario que luchemos contra la sociedad de la vigilancia y que nos resistamos a la introducción de nuevas tecnologías que se utilizarán para controlarnos individualmente y como colectivo. Es importante tomar medidas para defendernos de la vigilancia estatal y defender a los movimientos y comunidades que se llevarán la peor parte. Esto sólo es posible si somos capaces de mirar más allá de las cortinas de humo de la "seguridad nacional" del Estado, que pretenden aislarnos y dividirnos, y de solidarizarnos con los movimientos sociales radicales, las comunidades de la clase trabajadora y la gente de color, todos los cuales se enfrentan de forma desproporcionada a la represión y la criminalización del Estado.

RECOMENDACIONES

Es necesario defendernos a nosotros y a nuestras comunidades de la vigilancia estatal. Los sitios web que figuran a continuación ofrecen algunos ejemplos de cómo hacerlo:

- Privacytools.io ofrece servicios, herramientas y conocimientos para proteger su privacidad contra la vigilancia masiva global.
- La Electronic Frontier Foundation (eff.org) ofrece herramientas para proteger la privacidad digital y la libertad de expresión.

Si asiste a una protesta política, es probable que sea objeto de filmación y vigilancia policial. No es ilegal llevar una máscara en una protesta en el Reino Unido[198]. Echa un vistazo a este artículo sobre por qué la gente decide llevar una máscara en las manifestaciones como respuesta al aumento de la vigilancia policial - https://netpol.org/campaigns/protest-anonymity/

He aquí hay una serie de enlaces útiles a campañas contra diferentes aspectos del estado de vigilancia:

Network for Police Monitoring (https://netpol.org/), Big Brother Watch (https://bigbrotherwatch.org.uk/) y Privacy International (https://www.privacyinternational.org/) son excelentes recursos para monitorizar y hacer campaña contra el estado policial.

La campaña de Big Brother Watch sobre la tecnología de reconocimiento facial (https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/).

El trabajo del Undercover Research Group sobre el espionaje policial (https://undercoverresearch.net).

- Campaña de Netpol sobre la vigilancia de las protestas en el Reino Unido (https://netpol.org/campaigns/protest-surveillance/) e información útil "conozca sus derechos" para tratar con la policía (https://netpol.org/know-your-rights/).
- Corporate Watch (corporatewatch.org) tiene información útil sobre cómo hacer campaña contra el poder empresarial. También han publicado una guía para investigar a las empresas.

198 Las máscaras son legales a menos que un oficial de policía de alto rango ordene su retirada en virtud del artículo 60 de la Ley de Orden Público de 1994. Véase Free Beagles. '***Removal of Masks, etc***', https://network23.org/freebeagles/police-powers/removal-of-masks-etc/, [Accessed 16 March 2021].

La policía es el agente del Estado. Utiliza las tecnologías descritas en este informe para vigilarnos. Usted puede:

- Considera la posibilidad de crear un grupo "Copwatch" para defender a tu comunidad de la vigilancia estatal y la violencia policial. Véase https://wecopwatch.org/want-to-start-a-copwatch/
- Lea el llamamiento de Black Lives Matter para la desfinanciación de la policía (https://blacklivesmatter.com/what-defunding-the-police-really-means/).

Imágenes:

Portada:
Socialist Appeal_Protesta de Black Lives Matter. 6 de junio de 2020, Londres, Flickr

Portada interior:
Lucía Armiño

Página 3:
Fotomontaje. Imagen original Pxfuel.com

Página 15:
Fotomontaje. Imágenes originales Pxfuel.com

Página 25:
Pxfuel.com

Página 34:
Fotomontaje. Fuente: Wikipedia Commons

Página actual:
La multitud rodeando la estatua del esclavista Edward Colston durante la protesta de Black Lives Matter en Bristol. Keir Gravil. Flickr

SOBRE LAS ORGANIZACIONES

ENCO (European Network of Corporate Observatories) es una red de organizaciones cívicas y de comunicación europeas dedicadas a investigar las empresas y el poder empresarial.

https://corpwatchers.eu

Multinationals Observatory, con sede en París, es una plataforma online que ofrece recursos e investigaciones en profundidad sobre el impacto social, ecológico y político de las empresas transnacionales francesas.

https://multinationales.org

El Observatorio de Derechos Humanos y Empresas en el Mediterráneo (ODHE), con sede en Barcelona, es un proyecto de Suds y Novact que tiene como objetivo exponer el impacto y las complicidades de las empresas en materia de derechos humanos en contextos de ocupación y conflicto armado.

www.odhe.cat

Shoal es una cooperativa radical e independiente de escritores e investigadores. Producimos artículos de noticias, investigaciones, análisis y escritos basados en la teoría como una contribución y un recurso para los movimientos que intentan lograr el cambio social y político.

www.shoalcollective.org

En colaboración con:

NOVACT

suds Internacionalisme Solidaritat Feminismes

Con el apoyo de:

Ajuntament de Barcelona

ICIP Institut Català Internacional per la Pau

OPEN SOCIETY FOUNDATIONS