VIGILANCIA MASIVA Y CONTROL
DE LA DISIDENCIA EUROPEA

ESTADO ESPAÑOL

Vigilancia hi-tech en tiempos del COVID-19

Como las tecnologías digitales penetran en las esferas de seguridad pública y su impacto en las libertades civiles en el Estado español

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: Nora Miralles, Giulia Campisi y Carlos Díaz (ODHE)

Edición: Lina M. González y Felip Daza

Diseño: Lucía Armiño

Traducción: María Fernández

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

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

Barcelona / Abril 2021

AGRADECIMIENTOS

Queremos agradecer a todas las personas que han accedido y han mostrado disposición a hablar con nosotros y compartir su historia, incluso aun cuando esta no era agradable. También agradecemos especialmente a todos los que han sufrido directamente las prácticas de vigilancia que describimos en esta investigación.

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

Nuestra investigación presenta una visión general de la vigilancia masiva en España, centrándose en el uso de la tecnología contra activistas, comunidades o grupos determinados y otros actores políticos. Durante el proceso de investigación se han utilizado los siguientes métodos:

- Revisión de los perfiles corporativos en las bases de datos de empresas profesionales, de la prensa del sector y de la información facilitada por los periodistas, investigadores y grupos de campaña.
- Búsqueda en el Diario Electrónico de Licitaciones de la UE, en la página web de Licitaciones de España, en las páginas web de Licitaciones Regionales y en las páginas web de Licitaciones Locales.
- Búsqueda de contratos adjudicados por el Gobierno y los Fuerzas y Cuerpos de Seguridad del Estado.
- Entrevistas a activistas, abogados, expertos y otros miembros de la sociedad afectados por la tecnología.

INTRODUCCIÓN

Recientemente, han confluido dos tendencias que han contribuido en gran medida a ampliar la agenda digital del gobierno español, así como a normalizar las tecnologías que podrían utilizarse como medios de vigilancia masiva. Estos procesos están también alineados con la tendencia a recortar derechos y libertades en nombre de la seguridad nacional y el estrechamiento del espacio político de los ciudadanos facilita el uso de estas tecnologías para vigilar a grupos políticos disidentes.

Por un lado, el desarrollo de las ciudades para convertirlas en *Smart Cities* (ciudades inteligentes) es una de las soluciones que se presentan ante el imparable crecimiento de la urbanización y ante los numerosos retos que presenta en materia de seguridad ciudadana. Según las Naciones Unidas, el 55% de la población mundial reside actualmente en zonas urbanas. Se espera que esta cifra aumente hasta un 68% en 2050. **Este crecimiento ha llevado a pensar en soluciones para controlar y paliar los posibles problemas de superpoblación.**

La *Smart City* se convierte entonces en un sistema complejo que involucra a diferentes agentes. Cientos de miles de sensores se encuentran dentro de este sistema que mide varias cuestiones; desde la contaminación, las placas de los vehículos, hasta a la propia población.

En este sentido, las tecnologías de vigilancia y control desempeñan un papel clave en el sistema de una *Smart City*. Históricamente, el concepto de Seguridad Ciudadana ha sido una de las grandes aspiraciones y excusas para justificar la aplicación de medidas restrictivas. Ahora, bajo este concepto, la tecnología de vigilancia y control se ha instalado en todas partes con el fin de combatir la delincuencia; pero, al mismo tiempo, con el acceso en todo momento a observar y analizar todo lo que sucede en la ciudad.

Por otro lado, estas actividades potenciales de vigilancia masiva se ven reforzadas por la relación entre las empresas y los organismos públicos. Con el auge de la ideología neoliberal a finales del siglo pasado, la relación entre las instituciones públicas y el sector privado se intensificaron. Esta relación es crucial para comprender el fenómeno de la vigilancia masiva, no sólo porque son las empresas del sector privado las que proporcionan conocimientos y tecnología, sino también porque los datos que requieren los organismos gubernamentales para el control de la población proceden y se originan, en muchos casos, a través de las búsquedas en Internet, las interacciones en las redes sociales y las llamadas telefónicas. Esto hace **indispensable la relación entre las instituciones públicas y las empresas de ciberseguridad y tecnología.**

La llegada del COVID-19 parece apuntalar esta tendencia a la asociación público-privada, en la que el estado y el poder empresarial se unen para ejercer una nueva forma de control social en nombre de la salud y la seguridad pública, y utilizan la tecnología para transformar la vida privada en un sistema de dominación.

Del mismo modo, la pandemia ha supuesto un contexto prolífico para ampliar los usos de sistemas como el reconocimiento facial o la vigilancia con drones, que podrían estar ya afectando a la privacidad y pueden dificultar aún más el ejercicio de los derechos civiles y políticos. Su uso en manifestaciones y contra grupos disidentes es ya una realidad.

1 CONTEXTO: ESPAÑA COMO ESTADO DE VIGILANCIA

En los últimos años, el desarrollo digital ha sido fundamental para los sucesivos gobiernos españoles, al buscar convertir a España en uno de los países más "digitalizados" de la Unión Europea (UE). En 2019, la economía digital representaba el 19% del Producto Interior Bruto (PIB) español. Por eso, el gobierno comenzó a diseñar una Estrategia de Inteligencia Artificial y un ambicioso Plan Digital. Sin embargo, se ha prestado poca atención a la transparencia, la participación ciudadana y los derechos digitales y civiles. El enfoque de seguridad y el papel de las tecnologías en el contexto de la pandemia ha dado lugar a la profundización de un sistema de vigilancia digital.

Antes del estallido del COVID-19, el gobierno español ya estaba tomando medidas para convertir parte de su sistema de seguridad en un modelo de vigilancia masiva, mediante la aprobación del Real Decreto-Ley 14/2019 en octubre 2019. Esta ley, también conocida como "ley mordaza digital", permite al Estado -con independencia de la autorización judicial- intervenir en Internet y tomar el control de la infraestructura digital de determinadas entidades.

El Real Decreto Ley 14/2019 ha suscitado preocupación en la sociedad civil y entre Organizaciones No Gubernamentales (ONGs), como Amnistía Internacional, la cual denuncia que esta actividad *"se desarrolla en el marco de un procedimiento meramente administrativo, sin que exista un control judicial, para garantizar la supervisión del proceso"*[1]. Estas preocupaciones no parecen haberse tenido en cuenta ya que los mismos artículos polémicos del Decreto Ley aparecen también en el borrador de la nueva Ley General de Telecomunicaciones.

Otra medida legislativa es la Resolución de la Secretaría de la Presidencia, Relaciones con las Cortes y Memoria Democrática, aprobada en julio de 2020, que permite a los organismos encargados de hacer cumplir la ley instalar sistemas de reconocimiento facial en los puntos de acceso a eventos masivos, así como un sistema de detección de teléfonos móviles basado en la tecnología IMSI-catcher, con el objetivo de "proporcionar alertas a los agentes de seguridad para detener a las personas que tengan causas pendientes con la Justicia".

En julio de 2020, el Gobierno español presentó su agenda digital "España Digital 2025". Uno de los objetivos del plan es *"favorecer el tránsito hacia una economía del dato, garantizando la seguridad y privacidad y aprovechando las oportunidades que ofrece la Inteligencia Artificial, con la meta de que al menos el 25% de las empresas utilicen IA y Big Data en un plazo de cinco años"*, así como reforzar la ciberseguridad española[2].

1 Amnistía Internacional (2020) 'El Real Decreto Digital propicia la censura previa y el secuestro de contenidos en internet'. Disponible en: www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/el-real-decreto-digital-propicia-la-censura-previa-y-el-secuestro-de-contenidos-en-internet-por-part/

2 Plan España Digital 2025. Disponible en: www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf

El Gobierno español aprobó a principios de noviembre de 2020 la Orden PCM/1030/2020[3], en la que el Consejo de Seguridad Nacional establece un protocolo para actuar contra las *fake news*. Esta iniciativa se inspira en el Plan de Acción para la Democracia Europeo de la UE y en el Plan de Acción de la UE contra la Desinformación de 2018, creado con el fin de evitar la injerencia en las elecciones democráticas y la publicación de desinformación sobre las mismas. No obstante, esta Orden podría representar un ataque a la libertad de expresión, un derecho fundamental consagrado en la Constitución española, ya que la medida central del protocolo es la vigilancia continuada de las redes. Para cumplir con este plan nacional, el Gobierno ha creado una estructura en la que participan el Consejo Nacional de Seguridad, el Comité Especializado de Situación, la Secretaría de Estado de Comunicación, la Comisión Permanente contra la Desinformación y las autoridades públicas competentes, entre ellas la Presidencia, los gabinetes de comunicación de los ministerios y el Centro Nacional de Inteligencia (CNI). Esto demuestra una clara securitización de la información. La orden contempla la posibilidad de involucrar a los actores del sector privado que desempeñan un papel fundamental *"en la lucha contra la desinformación, con acciones como la identificación y no contribución a su difusión [...] y el desarrollo de herramientas para evitar su propagación [de la desinformación] en el entorno digital"*. La Orden no establece con claridad ni por qué ni cómo participarán los actores privados en el proceso de toma de decisiones en la lucha contra la desinformación, lo que ya ha suscitado preocupaciones sobre la independencia y la libertad de información.

Mientras tanto, la nueva Ley de Servicios Digitales de la UE, que está a punto de aprobarse, dará directrices europeas a todos los Estados miembros para abordar este tipo de políticas. Aunque la Ley no ha sido aprobada en el momento de la redacción de esta investigación, la Resolución aprobada por el Parlamento Europeo de octubre de 2020 en la que se remite a la Comisión de la UE sobre la futura Ley de Servicios Digitales, Resolución sobre la Ley de Servicios Digitales y cuestiones de derechos fundamentales (2020/2022(INI))[4], contiene recomendaciones y consideraciones de este tipo: *"considerando que un enfoque puramente autorregulador de las plataformas no proporciona la transparencia, la responsabilidad y la supervisión adecuadas; considerando que dicho enfoque no proporciona información adecuada a las autoridades públicas, a la sociedad civil y a los usuarios sobre la forma en que las plataformas abordan los contenidos y las actividades ilegales y los contenidos que violan sus términos y condiciones, ni sobre la forma en que curan los contenidos en general"*; y *"considerando que este enfoque puede no garantizar el cumplimiento de los derechos fundamentales y crea una situación en la que las responsabilidades judiciales se transfieren parcialmente*

3 Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional (2020). *BOE*. www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663

4 Motion for a European Parliament Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)). *European Parliament*. www.europarl.europa.eu/doceo/document/A-9-2020-0172_EN.html

a partes privadas, lo que plantea un riesgo de interferencia con el derecho a la libertad de expresión". Esto significa que ambas iniciativas del Gobierno español podrían considerarse una amenaza para el derecho a la libertad de expresión debido al importante papel que se les otorga a los actores del sector privado a la hora de determinar qué tipo de contenido constituye un discurso de odio, y quizás decidir y hacer campaña sobre lo que es desinformación o información.

Otro punto importante es que el Reglamento General de Protección de Datos de la UE (GDPR, por sus siglas en inglés)[5], establecido en 2016, regula todo el tratamiento de los datos personales en todos los Estados miembros. El Reglamento de la UE tiene por objeto proteger y garantizar el derecho fundamental a la información personal recogido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea[6]. En lo que respecta al tipo de datos que hay que proteger, el Reglamento enumera los datos biométricos, definidos como *"datos personales resultantes de un tratamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de dicha persona física, así como las imágenes faciales o los datos dactiloscópicos"*. Este es el tipo de datos que procesan las herramientas y tecnologías de vigilancia, como el reconocimiento facial. El artículo 9 del Reglamento establece que *"se prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, o datos biométricos destinados a la identificación inequívoca de una persona física, así como de datos relativos a la salud, la vida sexual o a la orientación sexual de una persona física"*. Los apartados posteriores establecen excepciones a esta prohibición, permitiendo el tratamiento de datos específicos en determinados casos, como cuando las personas dan su consentimiento, cuando no pueden dar su consentimiento explícito por motivos de salud y cuando *"g) El tratamiento sea necesario por razones sustanciales de interés público, sobre la base del Derecho de la Unión o de los Estados miembros, que deberá ser proporcional al objetivo perseguido, respetar la esencia del derecho a la protección de datos y prever medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses del interesado"*.

España adaptó el Reglamento de la UE en la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales[7], de diciembre de 2018, pero todavía no hay rastro de ninguna regulación sobre los datos biométricos. No obstante, existen algunos artículos dedicados a la regulación de los datos obtenidos mediante el uso de cámaras, en los que se señala que se permite su

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union.* eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

6 Charter of Fundamental Rights of the European Union. *Official Journal of European Communities.* www.europarl.europa.eu/charter/pdf/text_en.pdf

7 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018) *BOE.* www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

uso cuando sea necesario para salvaguardar la seguridad pública. Hay claras evidencias de que el pretexto de actuación en pro del interés público o la seguridad nacional se está utilizando cada vez más -y se está abusando de él- para permitir una vigilancia masiva que, de hecho, está conduciendo a una securitización de la sociedad.

Al mismo tiempo que intenta regular el entorno digital nacional, la UE parece haber estado "exportando" herramientas, capacitación y conocimientos en materia de vigilancia digital a países no miembros de la UE, en su mayoría de Europa del Este, Oriente Medio y del Norte de África, a través de diversos fondos y organismos de cooperación de la UE, en particular agencias de cooperación policial como la CEPOL. La organización Privacy International (PI) obtuvo acceso a varios documentos que muestran la experiencia europea en la exportación de la vigilancia digital, y la securitización de la migración como concepto[8], destacando un proyecto en Senegal, destinado a crear una base nacional de datos biométricos para "abordar las causas fundamentales de la migración irregular[9]", financiada por el Fondo Fiduciario de Emergencia de la UE para la estabilidad y el abordaje de las causas fundamentales de la migración irregular y del desplazamiento de personas en África (EUTF para Africa, por sus siglas en inglés)[10].

El Estado español contribuye a muchos de estos proyectos y programas de forma indirecta, a través de los organismos de la Unión Europea (principalmente en el ámbito de la gestión de las migraciones y las fronteras en el Magreb) y, de forma directa, a través de instituciones como la Policía Nacional, en la impartición de sesiones de formación sobre habilidades y tecnologías de vigilancia digital, tal y como ha descubierto Privacy International.

En Bosnia y Herzegovina, la Policía Nacional impartió una sesión de formación para la policía local y las autoridades de inteligencia sobre investigaciones financieras que "*esboza las posibles vías para el rastreamiento de direcciones IP, correos electrónicos y la realización de escuchas telefónicas*". Además, *"una diapositiva hacia el final de la sesión también promueve el uso de malware o troyanos informáticos -software utilizado para hackear dispositivos, extraer datos y tomar el control de funciones como la cámara y el micrófono, y vendido en el mercado abierto por empresas como NSO Group"*[11], mostrando claramente la forma en que esas prácticas de dudosa legalidad son comúnmente utilizadas y fuertemente recomendadas por las Fuerzas y Cuerpos de Seguridad del estado.

También ha habido preocupación por la privacidad en relación con las aplicaciones móviles desarrolladas por algunas regiones españolas para el rastreo de

8 Privacy International (2020) Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes. privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes

9 Termes de reference (2020). privacyinternational.org/sites/default/files/2020-11/Doc%203.3%20Annexe%20II%20Termes%20de%20r%C3%A9f%C3%A9rence%20SN.pd%20f.pdf

10 Document d'action du Fonds Fiduciaire de l'UE. ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-sah-ci-01.pdf

11 Privacy International (2020) 'Revealed: The EU Training Regime Teaching Neighbours How to Spy'. privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy

contactos de COVID-19: *"Hemos comprobado que estas aplicaciones están muy mal diseñadas desde el punto de vista del respeto a la privacidad. Son muy invasivas, ya que recogen datos que no son necesarios para el diagnóstico del coronavirus, comparten con Google y Facebook, e incluso con las PYMES que han desarrollado el software"* [12], afirma Gemma Galdón, analista de privacidad y directora de Eticas Consulting.

Al mismo tiempo, las empresas militares y de defensa, con el pretexto del COVID-19, se han mostrado dispuestas a hacer tratos con tecnologías de vigilancia y control. Según un informe de Amnistía Internacional, empresas como el Grupo Thales no están actuando con la debida diligencia para evitar que sus productos se utilicen en posibles violaciones de los derechos humanos e incluso en crímenes de guerra[13]. Thales y su subsidiaria Gemalto se encuentran entre las empresas que más se benefician de la militarización de las fronteras europeas[14]. Desde 2008, los laboratorios de Ciencia de Datos e Inteligencia Artificial de THALES han estado desarrollando un motor de simulación de multitudes llamado SE-Star, que permite gestionar y observar diferentes variables como factores motivacionales, emociones, estímulos, personalidades y comportamientos para controlar los flujos de multitudes[15]. En España, Thales ha suministrado al aeropuerto de Madrid tecnología de reconocimiento facial mediante un sistema biométrico llamado FRP (Face Recognition Platform)[16]. Estas empresas están aprovechando la pandemia para aplicar su tecnología, lo que también repercute en las libertades civiles. La lucha contra la pandemia del COVID-19 ha dado a los gobiernos la excusa perfecta para mostrar toda su fuerza de control, vigilancia y recopilación de datos en asociación con el sector privado.

12 V. Miró Julià (2020) 'Tecnologia mòbil contra el coronavirus: una amenaça per a la privacitat?' CCMA, 9 April. www.ccma.cat/324/tecnologia-mobil-contra-la-covid-19-una-amenaca-per-a-la-privacitat/noticia/3003525/

13 Amnesty International (2019) 'Arms companies failing to address human rights risks'. www.amnesty.org/en/latest/news/2019/09/arms-companies-failing-to-address-human-rights-risks/

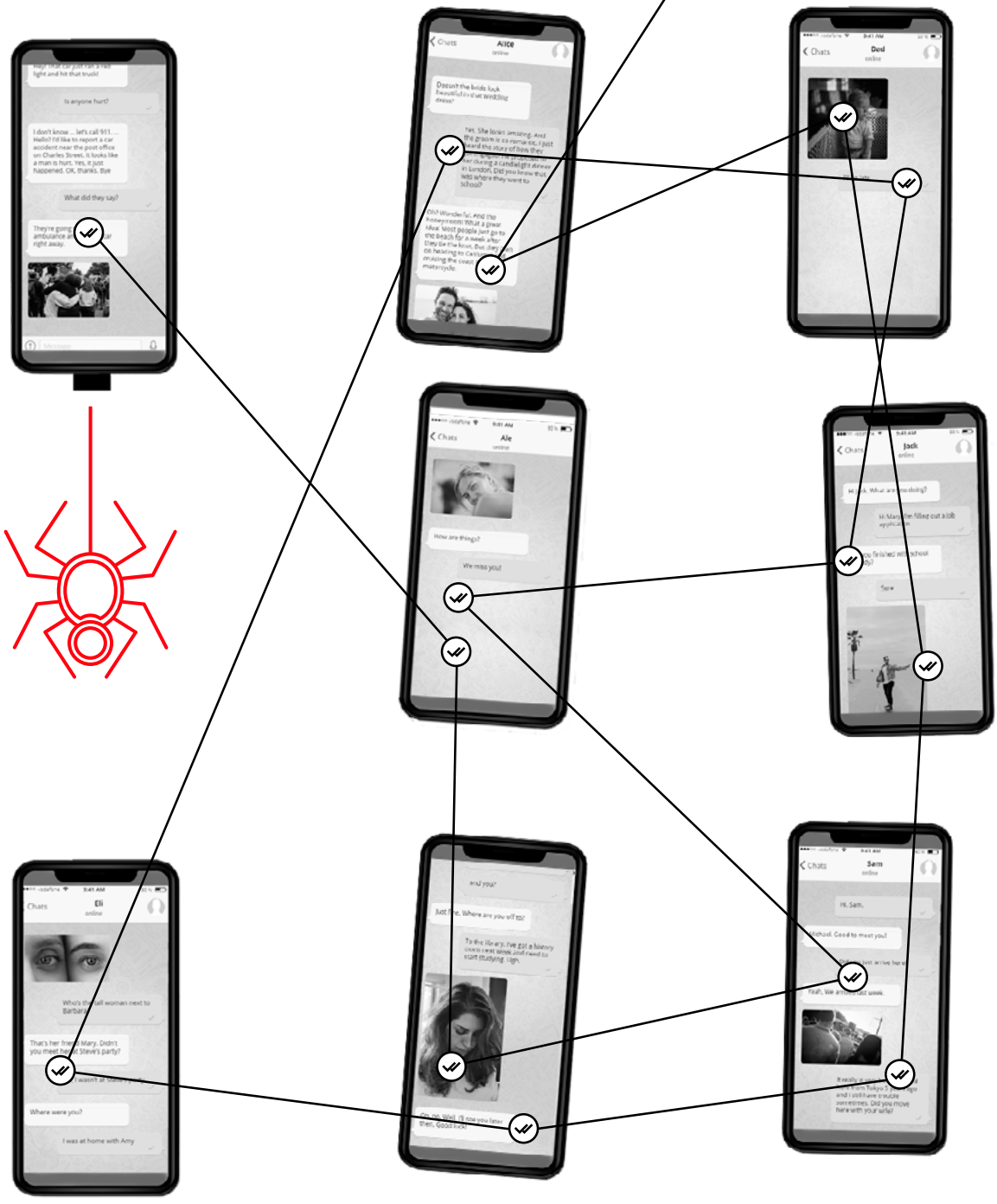
14 Thales Group website. 'Thales Gemalto EES Border Management System'. www.thalesgroup.com/en/markets/digital-identity-and-security/governmentgovernmentgovernmentgovernment/EES-border-management-system

15 European Project Driver +. SE-Star: THALES crowd simulation. https://pos.driver-project.eu/es/group/66

16 Computing (2020) 'FRP, la solución biométrica de Thales para contener a la Covid-19'. Disponible en: www.computing.es/mundo-digital/noticias/1119377046601/frp-solucion-biometrica-de-thales-contener-covid-19.1.html

Vigilancia hi-tech en tiempos del covid-19

2 TENDENCIAS



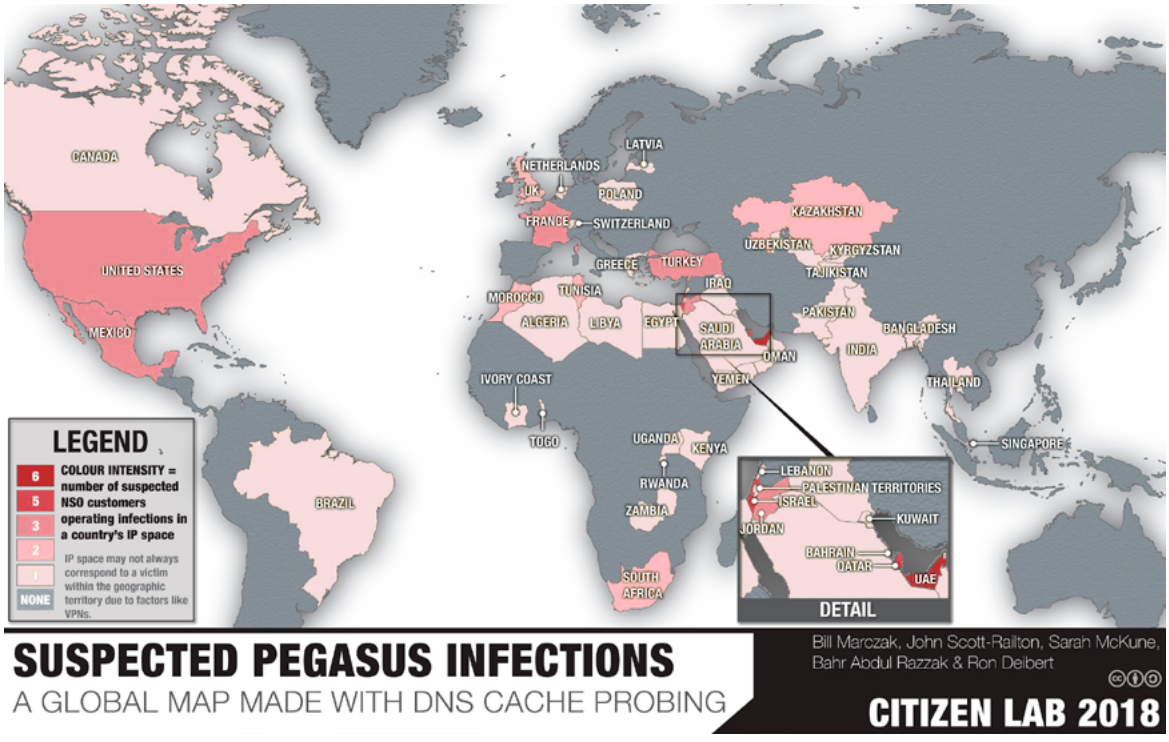
TENDENCIA 1:

HACKING GUBERNAMENTAL: infiltración digital y software espía

A mediados de 2020, una investigación de Citizen Lab sacó a la luz el uso del **Pegasus spyware** (un software espía) -vinculado a la empresa israelí NSO Group y adquirido por los servicios de inteligencia españoles en 2015- para espiar los archivos, fotografías, historial de navegación web, los correos electrónicos y otros datos de políticos independentistas catalanes. En respuesta a la pandemia, **NSO Group** ofreció a los Estados una nueva y gran herramienta de análisis de "big data" para mapear el movimiento de las personas y sus contactos, con el objetivo de ayudar a frenar el virus. Activistas y abogados han detectado recientemente la adaptación de técnicas clásicas, como la infiltración policial en el entorno digital mediante el uso de tecnologías *phishing* (la suplantación de identidad) e infiltración digital a través de redes de correo electrónico y mensajería como WhatsApp o Telegram.

EMPRESAS INVOLUCRADAS

NSO Group es una empresa israelí de ciberseguridad fundada en 2010 por Niv Carmi, Omri Lavie y Shalev Hulio, cuyos ejecutivos se cree que han servido en la Unidad de Inteligencia 8200 de Israel[17]. La empresa trabaja en la creación de programas informáticos de intrusión y vigilancia como **Circus y Pegasus**, que luego venden a instituciones gubernamentales, independientemente de su naturaleza. Se conoce que la Unidad 8200 utiliza métodos de vigilancia para espiar a la población palestina[18]. El *spyware* Pegasus permite leer mensajes, acceder a contenidos del móvil e incluso a activar en segundo plano componentes de este, como la cámara o el micrófono. Es una poderosa herramienta que aprovecha las vulnerabilidades críticas para atacar los teléfonos móviles a distancia. Según el centro de investigación canadiense CitizenLab, el programa espía se ha utilizado en al menos 45 países, entre ellos Bahréin, Emiratos Árabes Unidos y Arabia Saudí[19].



Mapa que muestra las afectaciones del spyware Pegasus. Fuente: Citizen Lab 2018

17 DW (2020) 'Israeli Spyware threatens to shut down abusers'. Disponible en: www.dw.com/en/israeli-spyware-firm-threatens-to-shut-down-abusers/a-52292492

18 J. Reed (2015) 'Unit 8200: Israel's cyber spy agency'. *Financial Times*, 10 July. www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

19 Citizen Lab (2018) 'Hide and Seek'. citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Según la revista *VICE*, la empresa israelí pudo entrar en el mercado español gracias a un contrato con el Gobierno español en 2015. Motherboard, la sección sobre Tecnología de VICE, pudo hablar con un antiguo empleado de NSO que declaró: "*en realidad estábamos muy orgullosos de ellos como clientes, finalmente un Estado europeo*"[20].

Circles es una empresa israelí de vigilancia que aprovecha los puntos débiles del sistema mundial de telefonía móvil para obtener toda la información personal y acceder a las llamadas, los mensajes de texto y la ubicación del teléfono en segundos, simplemente conociendo el número de teléfono y sin necesidad de hackearlo. Según sus empleados, se vende exclusivamente a los gobiernos. Circles está afiliado a la empresa israelí NSO Group, según declaró un portavoz a Motherboard: *"NSO y Circles son empresas separadas dentro de la misma familia corporativa, y ambas lideran sus industrias con un compromiso de negocio ético y se adhieren a estrictas leyes y regulaciones en cada mercado en el que operan"*[21]. El organismo canadiense de vigilancia de la ciberseguridad, Citizen Lab, ha descubierto que la actividad de Circles ha sido detectada en al menos 25 países[22]. La compañía emplea un sistema técnico conocido como **Sistema de Señalización 7 (SS7)**, que funciona cuando una persona viaja a otro país con su teléfono y la red SS7 lo traslada a otro proveedor de telecomunicaciones para ajustar la facturación. Circles obtiene las coordenadas de la torre de telefonía móvil más cercana al teléfono y es capaz de revelar su ubicación, así como acceder a sus datos y comunicaciones.

20 J. Cox & L. Franceschi (2020) 'Source: Spain is Customer of NSO Group'. Motherboard Tech by VICE, 14 July. www.vice.com/en/article/pkyzxz/spain-nso-group-pegasus-catalonia

21 J.Cox & L. Franceschi (2020) 'Researchers find powerful cellphone location surveillance in Europe, Middle East, Australia'. Motherboard Tech by VICE, 1 December. www.vice.com/en/article/wx8jax/researchers-find-powerful-ss7-cellphone-location-surveillance-in-europe-middle-east-australia

22 CitizeLab (2020) 'Running in Circles. Uncovering the clients of Cyberespionage firm Circles'. 1 December. citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

El uso de Pegasus para espiar a políticos independentistas

No es ningún secreto que el Estado español espió a políticos catalanes y activistas independentistas, al igual que a otros grupos políticos. Pero nada fue tan controvertido como la constatación de que los servicios de seguridad españoles estaban en posesión del programa espía conocido como **Pegasus**, desarrollado por la empresa israelí NSO Group.

En julio de 2020, Citizen Lab descubrió que los teléfonos móviles de varios políticos en España, y de otras 100 figuras de la sociedad civil del internacional, fueron atacados en 2019. Entre ellos, el del presidente del Parlamento catalán, Roger Torrent[23]. Todos fueron objetivo de Pegasus, teóricamente vendido a los Estados para luchar contra el crimen organizado y las redes terroristas; en cambio, utilizado por muchos gobiernos de todo el mundo para espiar a opositores políticos y periodistas. El teléfono de Torrent habría sido infiltrado a través de una llamada perdida a su WhatsApp en 2019. Inmediatamente acusó al Estado español de estar detrás del hackeo telefónico, ya que creía que probablemente se había producido sin una orden judicial[24]. Se trata del primer caso conocido de un Estado europeo que adquiere y utiliza Pegasus contra políticos electos.

Además de Torrent, investigadores del Citizen Lab de la Escuela Munk de la Universidad de Toronto -que colaboraron con Whatsapp tras descubrirse los supuestos intentos de hackeo- alertaron a otros dos políticos independentistas de que habían sido objeto de ataques en 2019: Ernest Maragall, exconsejero de Acción Exterior y también diputado del Parlament de Catalunya por el mismo partido independentista que Torrent[25], así como Anna Gabriel, ex diputada autonómica de la Candidatura de Unidad Popular (CUP)[26], partido anticapitalista y de extrema izquierda, que actualmente vive en Suiza tras huir de España para evitar ser encarcelada por promover presuntamente el referéndum del 1 de octubre de 2017.

23 S. Kirchgaessner and S. Jones (2020) 'Phone of top Catalan politician 'targeted by government-grade spyware''. *The Guardian*, 13 July. www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

24 X. Puig i Sedan (2020) 'Roger Torrent i Anna Gabriel espiats per una empresa que només treballa amb governs'. *El Temps*,14 July. www.eltemps.cat/article/10826/roger-torrent-i-anna-gabriel-espiats-per-una-empresa-que-nomes-treballa-per-governs

25 J. Gil (2020) 'El programa espía Pegasus atacó también el móvil de Ernest Maragall'. El País, 14 July. elpais.com/espana/2020-07-14/el-programa-espia-pegasus-ataco-tambien-el-movil-de-ernest-maragall.html

26 Swissinfo (14 July 2020) 'Investigación señala posible espionaje en el teléfono de Anna Gabriel'. www.swissinfo.ch/spa/politica/posible-espionaje-en-el-tel%C3%Agfono-de-anna-gabriel/45902840

En lo que respecta a los abusos cometidos mediante el uso de este software espía, los conocimientos tecnológicos adquiridos por los fundadores e ingenieros de la empresa en las unidades de inteligencia y defensa israelíes -se cree que sirvieron en la Unidad 8200 de Israel, que forma parte del mecanismo de control militar sobre los palestinos- se han desarrollado sobre las libertades civiles de las organizaciones y activistas palestinos bajo vigilancia[27]. Por este motivo, varias organizaciones de defensa de los derechos humanos han solicitado la revocación de la licencia de exportación de la empresa[28], en base a los múltiples casos de utilización de este software por parte de Estados que cometen graves violaciones de los derechos humanos.

Mail spoofing y phising para infiltrarse digitalmente en los movimientos sociales

En octubre de 2020, el periódico catalán *La Directa* hizo pública información relativa a técnicas de *Mail spoofing* (falsificación de correos) utilizadas en al menos 11 cuentas de correo electrónico de organizaciones políticas, movimientos juveniles, lugares de reunión comunitaria y sindicatos de vivienda[29]. Según los propios activistas, se enviaron más de 60 correos electrónicos falsos con el claro objetivo de recabar información sobre las actividades y documentos internos de estas organizaciones, y apuntando a algunos de los espacios políticos que actualmente movilizan más gente en España, como el movimiento independentista o el movimiento por el derecho a la vivienda. Para evitar que las direcciones IP fueran desenmascaradas, los usuarios que diseñaron este sistema utilizaron un servicio VPN, una herramienta que permite ocultar el número de identificación y la ubicación del dispositivo. Sin embargo, los periodistas que investigaron este escándalo tienen la certeza de que varias de las direcciones IP detectadas apuntan a la policía autonómica catalana, los Mossos d'Esquadra, y al Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Catalunya.

"Esta infiltración digital se produjo a través de la intromisión en el correo personal y en las cuentas corporativas de las organizaciones políticas, sin ninguna orden judicial ni autorización en caso de que esta infiltración proceda realmente de las fuerzas policiales", explica Eduardo Cáliz, quien forma parte del equipo jurídico que actúa en nombre de los activistas suplantados para llegar al fondo del asunto.

27 Who Profits (May 2020) NSO Group: Technologies of control. www.whoprofits.org/wp-content/uploads/2020/05/NSO-Pdf.pdf

28 Amnesty International (January 2020) 'Israel: Stop NSO Group exporting spyware to human rights abusers'. www.amnesty.org/en/latest/news/2020/01/israel-nso-spyware-revoke-export-license/

29 G. Garcia and J. Rodríguez (October 2020) 'Infiltrats dins la Pantalla', *La Directa* 510. https://directa.cat/que-hi-trobem-a-la-directa-510/

TENDENCIA 2:

VIGILANCIA DE AUDIO E IMAGEN EN ESPACIOS PÚBLICOS

El uso de la tecnología de videovigilancia (técnicamente CCTV, circuitos cerrados de televisión) en los espacios públicos es un mecanismo de control y vigilancia establecido en nuestra vida cotidiana. En España, las fuerzas del orden confían en la videovigilancia como herramienta para combatir la delincuencia y controlar el comportamiento de la población. Según un informe de Comparitech[30], la capital española se encuentra entre las cinco ciudades de la Unión Europea con mayor densidad de cámaras callejeras: Madrid tiene 4,42 dispositivos de cámara por cada 1.000 habitantes. Según Comparitech, sólo Berlín, Londres, Viena y Varsovia la superan. Hay un total de 29.000 cámaras de seguridad en todo Madrid.

30 P. Bischoff. 2020. 'Surveillance camera statistics: which cities have the most CCTV cameras?' Comparitech, 22 July. www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

EMPRESAS INVOLUCRADAS

CTRL4 ENVIRO[31] es una *startup* catalana que nació en 2006 de un proyecto de investigación junto con la Universidad Autónoma de Barcelona. La empresa está especializada en ofrecer medios de monitorización de movimientos de personas, así como en el seguimiento de los flujos urbanos. El COVID-19 ha sido el impulsor del diseño de una tecnología completamente nueva que permite vigilar a multitudes en espacios públicos, como las playas. Su producto **MDS** (Monitor de Distancia Social) es un sistema capaz de analizar anónimamente las imágenes ya disponibles de las cámaras de CCTV para controlar el distanciamiento social, el uso adecuado de la mascarilla y la densidad de ocupación, por ejemplo, en una de las playas más famosas de Barcelona[32].

SICE (Sociedad Ibérica de Construcciones Eléctricas, S.A), **empresa filial del Grupo ACS**[33], es una multinacional integradora de tecnología en el campo del tráfico y el transporte, el medio ambiente y la energía, las telecomunicaciones y diversos procesos industriales.

Uno de sus productos estrella son las cámaras de vigilancia. En 2015, SICE instaló 47 nuevas cámaras de vigilancia en el centro de Madrid, diez de las cuales incluyen un innovador software de análisis que alerta a la policía si detecta ciertos comportamientos "extraños", como un grupo de personas corriendo, permitiendo una intervención más rápida de la policía.

Las imágenes captadas por las cámaras se distribuyen a través de una red propia de fibra óptica que conecta de forma segura la cámara con la sede de la Policía Municipal y el Centro Integral de Señales de Vídeo (CISEVI). El visionado de este material está restringido a un grupo de policía municipal específicamente autorizado, y se almacena durante un máximo de siete días, tras los cuales se produce un borrado si no son reclamadas por la policía o un juez.

31 Company website. ctrl4enviro.com

32 Apte (2020) 'Ctrl4 Enviro controla el aforo de la playa de Castelldefels'. www.apte.org/ctrl4-enviro-controla-aforo-playa-castelldefels

33 SICE (2015) 'SICE installs 47 new surveillance cameras in the downtown area of Madrid'. www.sice.com/en/news/sice-installs-47-new-surveillance-cameras-downtown-area-madrid

Otro contexto operativo en el que la videovigilancia desempeña un papel importante es en las fronteras del país. En España, varias empresas se han beneficiado de los "negocios fronterizos". En 2013, el Ministerio del Interior español adjudicó un contrato para la instalación de 42 dispositivos de videovigilancia a lo largo de los casi 12 kilómetros de valla que separan la ciudad autónoma de Melilla de Marruecos[34]. Según la agencia de noticias *EFE*, fuentes de la Delegación del Gobierno en Melilla informaron de que la empresa a la que se había confiado el proyecto era **Cobra Instalaciones y Servicios S.A.**, filial del **Grupo ACS**.

A principios de 2019, el Consejo de Ministros de España aprobó un Plan de Medidas para el Refuerzo y la Modernización del Sistema de Protección Fronteriza Terrestre en Ceuta y Melilla. Una de las medidas es la instalación de un nuevo sistema de CCTV en el perímetro fronterizo de Ceuta que incluye 66 cámaras. El plan también promueve la instalación de sistemas de reconocimiento facial en los puestos fronterizos de El Tarajal (Ceuta) y en varias localidades de Melilla[35], donde al parecer Gunnebo y Thales están conversando con el Ministerio del Interior español para desarrollar el proyecto[36].

34 ABC España (2013. 'Interior refuerza la frontera de Melilla'. 10 January. www.abc.es/espana/20130110/abci-frontera-melilla-201301101339.html

35 La Moncloa (2019) 'Refuerzo y modernización del sistema fronterizo'. www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/180119-enlaceceutaymelill.aspx

36 El Faro de Ceuta (2019) 'La Frontera Inteligente'. 23 September. elfarodeceuta.es/frontera-camaras-reconocimiento-facial/

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

La expansión de las cámaras de videovigilancia en el centro de las ciudades como medida de seguridad pública con el pretexto de prevenir la delincuencia coincide con los procesos de gentrificación de algunas de estas áreas, que también resultan ser aquellas donde suelen tener lugar manifestaciones multitudinarias. El uso de sistemas cada vez más sofisticados de detección y análisis de comportamiento en estos dispositivos CCTV, ubicados en zonas públicas, alerta de una invasión cada vez más pronunciada a las libertades civiles, como el derecho a la privacidad y a la movilidad.

El aumento del control social en los espacios públicos a través de dispositivos de CCTV coincide también con el despliegue de la videovigilancia en aquellos barrios con una alta incidencia de tráfico de drogas, robos y otras actividades delictivas, como Lavapiés -donde se instalaron 48 cámaras de CCTV para vigilar toda la zona desde la plaza de Tirso de Molina hasta la Glorieta de Embajadores -epicentro de la movilización política[37]- y Vallecas. Ambas zonas madrileñas son barrios muy movilizados políticamente donde existen, por ejemplo, fuertes movimientos contra los desahucios, grupos de migrantes organizados y grupos antifascistas; y donde periódicamente se realizan operaciones policiales contra disidentes políticos y migrantes. De este modo, este tipo de tecnología puede utilizarse no sólo como elemento para disuadir la actividad delictiva, sino que también implicar un obstáculo al derecho de movilidad y el legítimo derecho a la protesta.

La abogada Laia Serra subraya los problemas jurídicos y éticos que plantea el carácter cada vez más sofisticado de la vigilancia y se pregunta: *"¿Por qué los ayuntamientos quieren cámaras con sistemas de reconocimiento tan avanzados, si su única misión es, en teoría, prevenir o evitar incidentes?"*.

En muchos otros casos, los CCTV y los videosensores se despliegan en barrios con una alta población o afluencia de inmigrantes y personas racializadas, lo que permite que los dispositivos contribuyan a la elaboración de perfiles raciales y, en su consecuencia, a la deportación. Esto ha sido denunciado por organizaciones como Irídia y Novact en un reciente informe[38]. En la misma línea, en Ciutat Vella, uno de los distritos de Barcelona donde se realizan más controles de identidad basados en el perfil racial, se iban a instalar trece dispositivos de videovigilancia para el 2020 con el fin de "garantizar la seguridad en los espacios públicos y contribuir a la lucha contra el terrorismo"[39].

37 Nodo50 (27 September 2009) 'Nos espían: 48 cámaras de videovigilancia serán instaladas en el barrio de Lavapiés y Tirso de Molina'. info.nodo50.org/Nos-espian-48-camaras-de.html

38 Irídia and Novact (October 2020) Report: 'Vulneraciones de los derechos humanos en las deportaciones'. iridia.cat/wp-content/uploads/2020/11/Deportaciones_FinalMOD_Imprimir-2.pdf

39 *Tot Barcelona* (16 May 2020) 'Barcelona encarrega 13 càmeres de vigilància al carrer a l'empara d'un programa antiterrorista'. www.totbarcelona.cat/societat/barcelona-encarrega-13-cameres-vigilancia-carrer-empara-programa-antiterrorista-54248/

El uso de la videovigilancia en los espacios públicos también puede utilizarse para vigilar actividades concretas de grupos políticos sin orden judicial. Especialmente las que rodean los locales políticos y centros sociales okupados, muy numerosos en ciudades como Madrid, Barcelona y Bilbao. Un caso claro de videovigilancia dirigida a grupos políticos se da en torno a la emblemática okupa Kasa de la Muntanya en Barcelona, una de las más antiguas de Europa. Hay varios dispositivos CCTV en la calle que permiten controlar las entradas a la casa donde se suelen celebrar reuniones políticas con gente de toda la ciudad. En 2013, activistas de la casa okupa informaron de haber descubierto y desmantelado una cámara de vídeo instalada frente a la casa, que estaba escondida en un falso tubo de ventilación del tejado de un hospital y era capaz de enviar las grabaciones a través de conexión wifi[40]. *"Las imágenes captadas por una cámara de videovigilancia pueden ser utilizadas en un sumario si cumplen con las formalidades de la ley que regulan su uso, pero a veces no se exige una autorización expresa para vigilar las actividades políticas, lo que vulneraría la regulación de estos dispositivos y las libertades civiles"*, afirma Eva Pous, abogada de la organización Alerta Solidària.

40 Squat!net (7 October 2013) 'Barcelona: Comunicat Kasa de la Muntanya. Després del desmuntatge d'un dispositiu de videovigilància'. Disponible en : ca.squat.net/2013/10/17/barcelona-comunicat-kasa-de-la-muntanya-despres-del-desmuntatge-dun-dispositiu-de-videovigilancia/

TENDENCIA 3:

INTERCEPTACIÓN DE COMUNICACIONES Y EXTRACCIÓN DE DATOS POR LOS ORGANISMOS DE APLICACIÓN DEL ORDEN Y LA LEY

Las fuerzas del orden destinan una parte importante de su presupuesto anual en tecnología de vigilancia para rastrear, localizar, vigilar y escuchar a la población española, a menudo con la mira puesta en los disidentes e inmigrantes. Uno de los métodos más utilizados para recopilar información es la extracción de datos de dispositivos personales, como teléfonos móviles, tabletas y ordenadores. Las tecnologías de extracción de datos de los teléfonos móviles, conocidas también como técnicas de análisis forense de teléfonos móviles, "requieren de una conexión física entre el dispositivo móvil que se quiere analizar y un dispositivo que extrae, analiza y presenta los datos contenidos en el teléfono", según Privacy International[41]. Las medidas para extraer y retener los datos de los teléfonos móviles y otros dispositivos constituyen una vulneración del derecho fundamental a la privacidad. Como tales, deben cumplir una serie de requisitos mínimos que

41 Privacy International (2019) 'A technical look at Phone Extraction'. privacyinternational.org/long-read/3256/technical-look-phone-extraction

garanticen el respeto de las normas internacionales de derechos humanos. Sin embargo, mientras que por un lado se detecta una tendencia estatal y regional que conduce a los gobiernos y proveedores de servicios a acumular cada vez más información sobre los usuarios; por otro, son empresas controvertidas las que poseen el monopolio de estos sistemas de extracción de datos, decodificación y análisis forense digital. Un ejemplo de ello es la israelí **Cellebrite**, cuya tecnología Universal Forensic Extraction Device (UFED) es utilizada por muchos cuerpos policiales europeos, incluidos los cuerpos de policía nacional y regional de España.

Por ahora, las técnicas más utilizadas siguen siendo los "cables policiales", ya sea el hackeo del micrófono de los teléfonos móviles o la colocación de micrófonos físicos en los locales. Por ejemplo, el Sistema Integrado de Interceptación de Telecomunicaciones (**SITEL**)[42] es un sistema informático integrado para la interceptación legal de las telecomunicaciones a nivel nacional y de uso conjunto por la Dirección General de Policía y la Guardia Civil, con dos centros de vigilancia y sus redes y terminales remotos asociados.

La Policía Nacional utiliza **SITEL**[43], para investigar miles de llamadas y mensajes después de su autorización judicial, a fin de obtener información en tiempo real sobre los interlocutores, el contenido, los mensajes y la ubicación. Este dispositivo puede grabar todas las conversaciones y las almacena en un disco duro. Todo está encriptado, de modo que sólo se puede acceder a SITEL mediante una clave personal.

42 La Información (2009) 'SITEL, el cuestionado sistema de escuchas del Gobierno'. 5 November. www.lainformacion.com/espana/sitel-el-cuestionado-sistema-de-escuchas-del-gobierno_tPhjJsRpvFCwBxAkbL0l7/

43 O. López-Fonsec (2020) 'Interior gasta 15 millones al año en su sistema de espionaje de comunicaciones'. El Pais, 17 July. elpais.com/espana/2020-07-16/interior-gasta-15-millones-al-ano-en-su-sistema-de-espionaje-de-comunicaciones.html

EMPRESAS INVOLUCRADAS

Insikt Intelligence es una empresa tecnológica con sede en Barcelona. Su objetivo es crear herramientas fáciles de usar para ayudar a los Fuerzas y Cuerpos de Seguridad del Estado a obtener información sobre la ciberdelincuencia. Son expertos en minería de redes sociales y en análisis de textos avanzados en todas las fuentes digitales, con más de una década de experiencia en investigación y desarrollo.

Insikt ha desarrollado una plataforma de inteligencia llamada **INVISO**, para la detección en tiempo real de radicales yihadistas en redes sociales.

Esta empresa catalana ha sido financiada por el Programa Horizonte 2020, con un proyecto llamado "Nueva plataforma de minería de datos sociales para detectar y vencer la radicalización violenta en línea"[44]. El proyecto tiene como objetivo anticiparse a los actos terroristas y luchar contra la radicalización, por lo que, para ello, resulta fundamental detectar la ciberpropaganda en una fase temprana. Este proyecto se desarrollo entre octubre de 2017 y marzo de 2020.

Insikt también participó en otro proyecto financiado con fondos europeos denominado "RED-Alert"[45], en el que se utiliza Inteligencia Artificial (IA) para recopilar, procesar, visualizar y almacenar datos en línea relacionados con presuntos terroristas. En este proyecto participó el Ministerio del Interior español a través de la Guardia Civil.

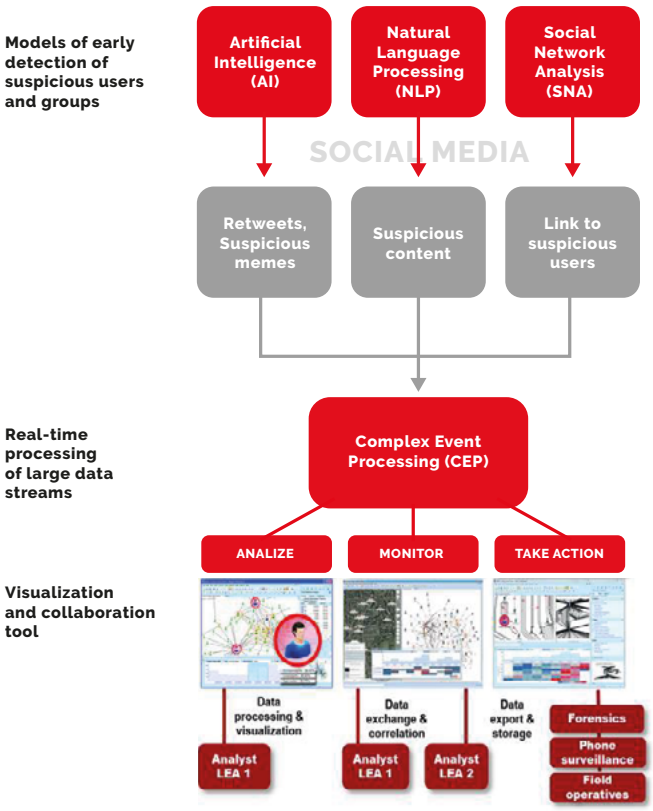
El consejo asesor del proyecto[46] incluye a varios especialistas, entre los que se encuentran los antiguos jefes de los servicios de inteligencia europeos, así como el antiguo director del Departamento de Seguridad, que posteriormente se convirtió en el Director de la Interpol y Operaciones Internacionales de la Policía Nacional de Israel (INP).

44 Horizon (2020) European Project. Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization. cordis.europa.eu/project/id/767542

45 Horizon 2020. European Project. Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing. cordis.europa.eu/project/id/740688

46 Horizon 2020. European Project. *Red Alert.* http://redalertproject.eu/about_us/advisory-board/

Diagrama muestra el proceso de trabajo del Proyecto RED-Alert. Fuente: RED-Alert Project.



Otro proyecto en curso financiado por el Proyecto Horizonte 2020 es el de Predicción e Inteligencia Visual para la Seguridad de la Información – PREVISION[47], en el que participan varios organismos públicos y actores privados españoles. El proyecto comenzó en septiembre de 2019 y se extenderá hasta agosto de 2021, con una financiación de la Unión Europea de 8 millones de euros.

PREVISION proporcionará soporte analítico avanzado y casi en tiempo real para múltiples flujos de big data (procedentes de redes sociales en línea, Internet, la "Dark Web", sistemas de CCTV y videovigilancia, fuentes de datos de tráfico y de datos financieros). En el proyecto también hay participación española, como la Universidad Politécnica de Valencia, el Departamento de Seguridad del País Vasco y la empresa privada **ETRA**.

47 Horizon 2020. European Project. PREVISION Prediction and Visual Intelligence for Security Information. cordis.europa.eu/project/id/833115

Fortier Europe es un distribuidor en España y Suiza de equipos profesionales de alta gama de audio, vídeo y telecomunicaciones. Su clientela en España son principalmente Fuerzas y Cuerpos de Seguridad del Estado. Algunos de los productos que la empresa comercializa en España están etiquetados como "probados en terrorismo". Esta empresa ha obtenido numerosos contratos públicos en la última década[48] para el suministro de cuatro equipos de audio encubierto micro-IP con equipos de comunicación IP[49], de equipos de rastreo GPS, y un equipo de grabación de audio encubierto[50]. Fortier Europe se ha asociado con Cedar Surveillance para vender sus productos a las fuerzas de seguridad de España. Cedar Audio es una empresa británica especializada en productos de audio, pero también produce sistemas de audiovigilancia, como el Trinity System[51].

La Unidad Central Operativa de la Guardia Civil[52] dispone de un sistema denominado **Egobox** fabricado por Fortier Europe S.L.. Este sistema permite la grabación discreta de audio, así como también es capaz de grabar conversaciones a larga distancia. Egobox funciona en paralelo con SITEL, también utilizado por la Guardia Civil.

Grupo Excem es una empresa multinacional cuya sociedad matriz (con sede en España) se dedicaba originalmente al suministro de cemento para la construcción, y es ahora un conglomerado empresarial con presencia en España, China, Francia, Israel y Estados Unidos bajo el nombre de Excem Grupo 1971, S.A..

Excem también colabora con las Fuerzas Armadas españolas, especialmente en el mantenimiento de equipos de interceptación de telefonía móvil. El contrato está valorado en 347.645 euros y fue negociado en secreto, según ha informado *El Confidencial Digital*[53].

Según fuentes consultadas por *El Confidencial Digital*, el mantenimiento se realiza al **Sistema Verint**, desarrollado por la empresa israelí-estadounidense **Verint**. Este sistema permite a cualquier organismo de aplicación de la ley utilizar herramientas portátiles para "interrogar" a las líneas de telefonía móvil y determinar, entre otras cosas, quién es su propietario, dónde se encuentra o extraer datos de un dispositivo.

48 Infocif. Fortier Europe S.L. Profile. www.infocif.es/licitaciones/fortier-europe-sl

49 Contractació Pública de la Generalitat de Catalunya. contractaciopublica.gencat.cat/ecofin_pscp/AppJava/awardnotice.pscp?reqCode=viewPcan&idDoc=69936170&lawType=3

50 Contractació Pública de la Generalitat de Catalunya. contractaciopublica.gencat.cat/ecofin_pscp/AppJava/awardnotice.pscp?reqCode=viewDcan&idDoc=23600769&lawType=2

51 Company Website. Surveillance products. www.cedar-audio.com/products/trinity/portablesurveillance.shtml

52 Portal de la Transparencia (2017) Adquisición de sistemas discretos de grabación de audio para la ampliación del sistema EGOBOX del que dispone la Unidad Central Operativa de la Guardia Civil. transparencia.gob.es/servicios-buscador/contenido/contratolicitacion.htm?id-Licitacion_33fd769e43c92cf17f81a61a23f94f66fd38c25b&fcAct-2017-06-26T17:59:20.898Z&lang-es

53 El Confidencial Digital (2017) 'El Ejército de Tierra subcontrata el mantenimiento de su sistema de escuchas telefónicas'. ECD, 17 January. www.elconfidencialdigital.com/articulo/defensa/Ejercito-Tierra-subcontrata-mantenimiento-telefonicas/20170116184112084093.html

Verint se hizo famosa en España en 2012 cuando sus productos fueron presuntamente utilizados por la empresa Interligare para espiar a los líderes políticos del Partido Popular[54]. Según un informe de Privacy International, Verint vendió junto a otra empresa israelí, NICE Systems[55] en 2014 tecnologías de vigilancia altamente desarrolladas a Kazajistán y Uzbekistán.

A nivel regional, y dadas las competencias en seguridad pública de los Mossos d' Esquadra, la policía catalana adquirió un sistema fabricado por Excem[56] que le permite interceptar y monitorear las comunicaciones[57]. Se trata de uno de los mayores contratos de Departamento de Interior de la Generalitat de Catalunya, por valor de varios millones de euros. El Departamento de Interior ha llamado a este sistema *Sistema d'intercepció legal de les comunicacions* (**SILTEC**).

Las comunicaciones interceptadas por el Departamento de Interior catalán se han hecho con tecnología suministrada por la empresa Excem, también proveedor de SILTEC y es responsable de su mantenimiento desde 2010. Excem también aprovisionó con dos equipos portátiles de interceptación móvil Verint, que supuestamente habrían sido adquiridos por los Mossos hace algunos años.

S21Sec es una de las primeras empresas de ciberseguridad con operaciones y oficinas en Portugal y España. En su página de LinkedIn, define su negocio como la mayor empresa *ibérica* de ciberseguridad[58]. La firma participó junto a la policía de Cataluña en el proyecto europeo CAPER[59], cuyo objetivo era crear una plataforma común para la prevención de la delincuencia organizada mediante el intercambio, la explotación y el análisis de fuentes de información abiertas y privadas.

El proyecto CAPER fue apoyado por la Comisión Europea a través del Séptimo Programa Marco de Investigación y Desarrollo Tecnológico (7PM) con hasta 5,6 millones de euros, de un presupuesto total de 7,1 millones. El proyecto, de tres años de duración, finalizó en 2014.

54 El Confidencial Digital (2012) 'El 'watergate español' incluye seguimientos a altos cargos del PP mediante maletas espía G12. 'Interligare' reunió datos sobre dirigentes como Alberto Ruiz-Gallardón'. ECD, 9 August. www.elconfidencialdigital.com/articulo/politica/PP-G12-Interligare-Alberto-Ruiz-Gallardon/20120809010000066200.html

55 B. Bryant (2014) 'US and Israeli Companies Are Selling Surveillance Technology to Repressive Regimes, Report Finds' VICE, 20 November. www.vice.com/en/article/pa89bn/us-and-israeli-companies-are-selling-surveillance-technology-to-repressive-regimes-report-finds

56 Contractació Pública de la Generalitat de Catalunya. contractaciopublica.gencat.cat/ecofin_pscp/AppJava/awardnotice.pscp?reqCode=viewPcan&idDoc=69936170&lawType=2

57 Contractació Pública de la Generalitat de Catalunya. contractaciopublica.gencat.cat/ecofin_pscp/AppJava/awardnotice.pscp?reqCode=viewDcan&idDoc=36543330&lawType=2

58 Company's profile on LinkedIn. www.linkedin.com/company/s21sec/?originalSubdomain=es

59 European Commission-funded *CAPER PROJECT*. www.fp7-caper.eu/

A través del Centre de Telecomunicacions i Tecnologia de la Generalitat de Catalunya, los Mossos d' Esquadra adquirieron un sistema fabricado por la empresa israelí **Voyager Labs**[60] y distribuido en España por S21Sec, que se basa en la IA para llevar a cabo estrategias de investigación de amenazas en Internet enfocadas a combatir el terrorismo yihadista[61]. El contrato comenzó en julio de 2020, por lo que las consecuencias se conocerán en un futuro próximo. El contrato se hizo mediante un procedimiento de "emergencia" -es decir, sin abrir ninguna licitación ni permitir que otra empresa se presente- alegando "razones de seguridad nacional", según consta en el expediente[62].

Según su página web, uno de sus productos clave es **Voyager Analytics**[63], un sistema capaz de analizar "inmensas cantidades de datos" para determinar las redes de relaciones, el comportamiento y las preferencias de un individuo concreto, los intereses de un grupo, sus vínculos y miembros, el papel que desempeña cada uno, las figuras clave de los acontecimientos y el grado en que todo esto puede constituir una amenaza.

La otra tecnología desarrollada por la empresa se llama **Voyager Check**[64], y utiliza algoritmos de aprendizaje automático y lenguaje natural para generar alertas o responder a preguntas específicas. La compañía dice que permite una respuesta "casi en tiempo real" incluso si se trata de información de millones de personas.

La compañía está en expansión, y en mayo de 2019 inauguró su nuevo centro de operaciones de seguridad en Madrid, desde donde toda esta actividad e incidentes de ciberseguridad que ocurren dentro y fuera de España se monitorearán en tiempo real[65].

60 E. Borràs (2020) 'El Govern destina 1,5 milions en un sistema per espiar el jihadisme a la xarxa'. *Diari Ara*, 18 August. www.ara.cat/societat/Govern-Mossos-plataforma-tecnologica-inteligencia-criminal-emergencia-seguretat-nacional-terrorisme-jihadista_0_2510149101.html

61 Contractació Pública de la Generalitat de Catalunya. contractacionpublica.gencat.cat/ecofin_pscp/AppJava/ca_ES/awardnotice.pscp?idDoc=66289761&reqCode=viewPcan

62 Centre de Telecomunicacions i Tecnologies de la Informació. Resolució de rectificació d'inici de l'execució. *Diari Ara.* www.ara.cat/2020/08/17/08_2020196L00_RE_inici_exec_rectifv3_-1.pdf?hash=69e1612369ad23aba4d41fd41ac00ee7e76db23f

63 Company Website. voyageranalytics.co/

64 Product's website. Online: voyageranalytics.co/solutions/voyagercheck/

65 S21sec (2019) S21sec inaugura su nuevo soc en madrid, una referencia para la ciberseguridad en Europa. www.s21sec.com/2019/08/13/s21sec-inaugura-su-nuevo-soc-en-madrid-una-referencia-para-la-ciberseguridad-en-europa-2/

Cellebrite es una empresa líder en análisis forense digital fundada en 1999 en Petah Tikva (Israel)[66], muy popular entre las agencias gubernamentales y los Estados. En la actualidad, la empresa es una filial de la japonesa **Sun Corporation**, aunque su sede y su equipo ejecutivo están situados en Israel. El dispositivo más extendido y famoso de la empresa, el UFED, es capaz de acceder y extraer datos explotando las vulnerabilidades de una amplia gama de dispositivos digitales para recopilar información como redes wifi, datos de localización y de la nube de móviles y dispositivos GPS. La extracción lógica del UFED de Cellebrite también puede recuperar datos eliminados, según se indica en su página web. La empresa israelí presta apoyo a fuerzas policiales nacionales y transnacionales -como el FBI[67], la Interpol[68] o la Europol-, servicios de inteligencia, patrullas fronterizas, fuerzas especiales y militares y organizaciones financieras de más de 100 países.

En línea con la estrategia de algunos países europeos que utilizan cada vez más la vigilancia de teléfonos inteligentes para controlar los movimientos de los solicitantes de asilo, Cellebrite ofrece su tecnología para auditar el viaje de una persona para identificar actividades sospechosas antes de su llegada, rastrear su ruta, ejecutar una búsqueda de palabras clave e imágenes a través de su dispositivo para identificar rastros de actividades ilícitas[69].

En el caso de España, Cellebrite ha sido utilizado por la Guardia Civil para hackear el teléfono de Josep Maria Jové, un político catalán detenido por la supuesta organización del referéndum del 1 de octubre y que se negó a dar su contraseña a los agentes[70].

66 Cellebrite website. 'About the company'. www.cellebrite.com/en/about/

67 J. Cox (2016) 'Meet Cellebrite, the Israeli Company Reportedly Cracking iPhones for the FBI'. *Motherboard (Vice)*, 23 March. https://www.vice.com/en/article/4xa3eq/meet-cellebrite-the-israeli-company-reportedly-cracking-iphones-for-the-fbi

68 Interpol (12 April 2016) 'INTERPOL agreement with Cellebrite strengthens efforts in combating cybercrime'. Online: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2016/INTERPOL-agreement-with-Cellebrite-strengthens-efforts-in-combating-cybercrime#:~:text=INTERPOL%20agreement%20with%20Cellebrite%20strengthens%20efforts%20in%20combating%20cybercrime,-12%20de%20abril&text=SINGAPORE%20%2D%20INTERPOL%20and%20Cellebrite%20have,global%20efforts%20to%20combat%20cybercrime

69 Privacy International (3 April 2019) 'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers'. https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

70 *El Español* (12 December 2017) 'La Guardia Civil tuvo que ir a Munich para desbloquear un móvil de Jové'. https://www.elespanol.com/espana/20171211/268724202_0.html

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

Interceptación policial *intrusive* y localización por GPS

La vigilancia de activistas por parte de las fuerzas policiales españolas está lejos de ser una simple anécdota. Sin embargo, algunos casos merecen una mención especial por su gravedad y sus consecuencias enormemente perjudiciales para el derecho a la privacidad y el secreto de las comunicaciones.

Entre 2013 y 2015, la Guardia Civil, la Policía Nacional y las policías autonómicas catalanas abrieron una serie de macrooperaciones contra grupos anarquistas, en las que fueron detenidas 68 personas. En diciembre de 2014, la primera operación, denominada en clave Pandora, se saldó con 11 detenciones en Cataluña y Madrid, registros domiciliarios y en locales políticos, y la incautación de libros, documentos, ordenadores y teléfonos[71]. Siete de los activistas permanecieron en prisión preventiva en Madrid durante seis semanas, acusados de pertenecer a un grupo terrorista de ideología anarquista, hasta que se levantó el sumario. Las pruebas se basaban en dos hechos: la posesión de un folleto titulado *Contra la Democracia* y "*el uso de medidas de seguridad extremas, como el servidor de Riseup*", en palabras del juez de la Audiencia Nacional que autorizó la orden[72]. A pesar de que la utilización de este servidor era completamente legal, la acción policial estigmatizó el uso de las comunicaciones encriptadas como medio de protección contra la vigilancia del Estado, haciendo ver que era una actividad delictiva.

71 J. Rodríguez (2015) 'Cas Pandora: un artefacte ideat pels serveis d'informació dels Mossos d'Esquadra'. *La Directa*, 29 October. https://directa.cat/cas-pandora-un-artefacte-ideat-pels-serveis-dinformacio-dels-mossos-desquadra/

72 Blog Buen Juicio (13 June 2015) ' Operación Pandora: ni usar PGP ni software de cifrado es un delito'. http://www.buenjuicio.com/operacion-pandora-ni-usar-pgp-ni-software-cifrado-es-un-delito/

En el caso de la Operación Pandora I y II, que fueron el resultado de una investigación de los Mossos d'Esquadra autorizada por la Audiencia Nacional, las personas detenidas habían sido sometidas durante mucho tiempo, algunas de ellas incluso durante años, a escuchas policiales especialmente invasivas y perjudiciales, vulnerando su derecho a la privacidad. Tras la absolución de los detenidos en ambas redadas, el juez alegó que *"las declaraciones genéricas realizadas carecen de una base objetiva sólida en el contenido de las conversaciones que se han facilitado"* [73]. Y añadía: *"a lo largo de la investigación, no se ha dado ninguna indicación sobre qué frases o conversaciones concretas podrían referirse a un acto terrorista específico"*. Una de las personas anarquistas detenidas en la primera Operación Pandora, que también estuvo en prisión preventiva durante casi dos meses, explicó a nuestros investigadores que -en su caso- se interceptaron 400 mensajes y 261 conversaciones telefónicas. La mayoría de las conversaciones eran de carácter íntimo o relacionadas con sus redes afectivas y de amistad.

Otro de los casos más recientes de escuchas policiales a disidentes políticos fue la investigación de los llamados Comités de Defensa de la República (CDR), grupos independentistas catalanes. El 23 de septiembre de 2019, la Guardia Civil detuvo a nueve personas -algunas de ellas activistas ecologistas o de asociaciones de vecinos- en varias localidades catalanas, con un gran despliegue de la policía antiterrorista[74]. Se les acusó de preparar acciones violentas contra el encarcelamiento de políticos y dirigentes independentistas. Según uno de los activistas, en algunos casos los policías encargados de investigarlos tenían copias de las llaves de sus coches y varios de ellos descubrieron también que se habían colocado dispositivos GPS en los vehículos para seguir sus movimientos[75]. Su abogado advierte: *"el hecho de que el sumario sea secreto nos impide valorar si este nivel de vigilancia con escuchas telefónicas, micrófonos, localización GPS, etc. estaba justificado, ya que no se sabe cómo se acuerdan estas medidas ni los motivos. Es una anomalía y un peligro para los derechos y las libertades"*.

En 2015, una activista por los derechos digitales denunció haber encontrado un dispositivo GPS pegado bajo su coche, tras ser detenida en un control policial de camino al Circumvention Tech Festival[76], irónicamente, una conferencia sobre vigilancia y privacidad en Valencia.

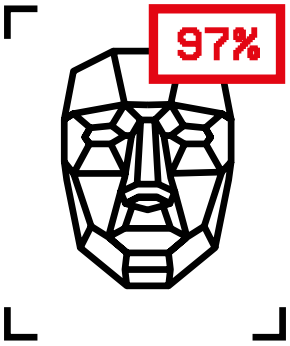
73 *Diari Ara* (15 June 2016) 'L'Audiència Nacional arxiva el cas dels activistes detinguts en l'operació Pandora II'. https://www.ara.cat/societat/Audiencia-Nacional-arxiva-investigacio-Pandora_0_1595840637.html

74 G. Liñá (2019) 'El Estado presiona al independentismo acusándolo de terrorismo en puertas de la sentencia'. *El Nacional,* 23 September. https://www.elnacional.cat/es/politica/estado-independentismo-terrorismo-sentencia_423032_102.html

75 J. Villarroya and J. Medina (2020) 'Els interessava molt poder relacionar l'independentisme amb la violència', interview. *El 9 nou*, 28 August. https://elgnou.cat/valles-oriental/actualitat/els-interessava-molt-poder-relacionar-lindependentisme-amb-la-violencia/

76 M. Gonzalo (2015) 'Cómo es el dispositivo rastreador que pusieron a la activista que fue a un congreso de privacidad'. ElDiario.es, 8 March. https://www.eldiario.es/turing/vigilancia_y_privacidad/dispositivo-rastreador-pusieron-activista-privacidad_1_4337571.html

TENDENCIA 4:



RECONOCIMIENTO FACIAL Y TECNOLOGÍA BIOMÉTRICA

Los algoritmos de reconocimiento facial tienen diferentes tasas de precisión según los grupos raciales, de acuerdo con un estudio publicado por el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) en 2019[77]. El NIST pudo confirmar que la mayoría de los algoritmos presentan diferencias demográficas tanto en las tasas de falsos negativos (rechazando una coincidencia correcta) como en las tasas de falsos positivos (coincidiendo con la persona equivocada). Empresas como Amazon e IBM están haciendo una pausa y abandonando su tecnología de reconocimiento facial después de años de presión de grupos de defensores de los derechos civiles[78].

77 NIST (2019) Study on Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

78 I. Ivanova (2020) 'Why face-recognition technology has a bias problem'. CBS News, 12 June. www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias/

La tecnología de reconocimiento facial se aplica en España en diversos escenarios, como las terminales de autobuses desde 2016[79], pero lo cierto es que se ha desplegado a una escala mucho mayor durante la pandemia de COVID-19.

En 2020, la Subsecretaría de Estado aprobó una Resolución en acuerdo con el Centro para el Desarrollo Tecnológico e Industrial (CDTI) para instalar cámaras de reconocimiento facial en la entrada de estadios, salas de conciertos y otros grandes recintos de toda España[80] .

La tecnología de reconocimiento facial se ha utilizado en diferentes contextos en España, incluidos los establecimientos comerciales donde se puede "pagar con la cara". Este sistema permite identificarte mediante el reconocimiento facial a través de la tecnología biométrica y puedes realizar automáticamente un pago que se cargará a la tarjeta de crédito con la que te registraste.

La tecnología de reconocimiento facial también ha llegado al mundo del automóvil. La compañía española **Grupo Antolín** y la israelí **Eyesight** han unido sus fuerzas para lanzar este sistema en los futuros vehículos. En esta alianza, la empresa española integra tanto sensores de vigilancia como cámaras que permiten que esta tecnología no sea invasiva. Por su parte, Eyesight desarrolla todo el software que permite el reconocimiento facial. Bajo el nombre de **Driver Sense**, este sistema de monitorización del conductor analiza los ojos, párpados, pupilas, la posición de la cabeza y la mirada del conductor para determinar su atención y alertarle de distracciones y somnolencia[81].

79 Algorithm Watch (11 August 2020) 'Spain's largest bus terminal deployed live face recognition four years ago, but few noticed'. http://algorithmwatch.org/en/story/spain-mendez-alvaro-face-recognition/

80 Boletín Oficial del Estado (2020) Resolution of 16 July 2020, of the Under-secretariat, publishing the Agreement between the Centre for the Development of Industrial Technology, E.P.E., and the Ministry of the Interior, regarding the pre-commercial procurement of R&D services in the field of security in rural areas. www.boe.es/diario_boe/txt.php?id=BOE-A-2020-8276

81 J.A. González (2020) 'El reconocimiento facial se mete en el coche para vigilar la fatiga'. *El Comercio*, 17 January. Online: www.elcomercio.es/tecnologia/reconocimiento-facial-coche-colaboracion-espana-israel-20200117095840-ntrc.html?ref=https:%2F%2Fwww.google.com%2F

EMPRESAS INVOLUCRADAS

Herta Security (Grupo Everis) es líder mundial en tecnología de reconocimiento facial e identificación de multitudes. Con sede en Barcelona y oficinas en Los Ángeles, Ciudad de México y Montevideo, Herta tiene socios en 50 países y más de 250 colaboradores certificados en todo el mundo. Herta security nació como un spin-off de la Universidad Politécnica de Cataluña. Algunos de sus proyectos incluyen ciudades seguras, aeropuertos, estaciones de tren y metro, prisiones, bancos, casinos, estadios deportivos, centros comerciales, aplicaciones militares, policiales y forenses. La empresa pertenece al Grupo Everis Aeroespacial, Defensa y Seguridad[82].

Herta se especializa en el análisis de entornos concurridos, lo que permite detectar e identificar a múltiples sujetos al mismo tiempo a través de cámaras IP.

La empresa es relativamente nueva, ya que inició sus actividades en 2009, pero su alcance internacional es sorprendente. Herta Security ha conseguido contratos públicos en España y en otros países del extranjero. Los controles fronterizos también han pasado a formar parte del negocio de la empresa catalana. Herta ha desarrollado un proyecto en Phuket destinado a identificar a las personas que acceden al país o a la ciudad en sus vehículos con el fin de reducir los índices de delincuencia[83]. En el puesto de control de seguridad, la policía utiliza sus teléfonos móviles para fotografiar a todos los pasajeros de los vehículos que llegan a la ciudad. A continuación, la transmisión de imágenes/vídeo se transfiere a través de un punto de acceso inalámbrico (AP) a la red del sistema "BioSurveillance NEXT" de Herta[84]. Cada vez que se detecta un sujeto en la lista negra, el sistema envía una alarma a los teléfonos móviles de los guardias de seguridad.

En España, los productos de Herta Security se utilizan en la mayor terminal de autobuses desde 2016[85]. Según la empresa, el sistema ha sido un éxito desde su implantación dada la reducción en un 75% de los incidentes[86].

82 Everis website. November 2017. 'Everis integrates biometrics facial recognition with Mirasys' Video Management Software'. https://www.everis.com/global/en/news/newsroom/everis-integrates-biometrics-facial-recognition-mirasys-video-management-software

83 Security World Market. December 2017. ' Herta wins biosurveillance contract in Phuket'. www.securityworldmarket.com/na/News/Business-News/herta-wins-biometrics-contract-in-phuket

84 Herta Security website. 'Case Study: Safe City in Asia'. Accessed 25/10/2020: http://hertasecurity.com/wp-content/uploads/Case-Study-SafeCity.pdf

85 Axis website. Customer story (2016) 'Estación sur de Autobuses de Madrid: Análisis de vídeo para la estación de autobuses con más tránsito de Europa'. Online: www.axis.com/es-es/customer-story/4443

86 N. Bellio (2020) 'Spain's largest bus terminal deployed facial recognition four years ago, but few noticed'. *Algorithm Watch*. Accessed 28/11/2020: algorithmwatch.org/en/spain-mendez-alvaro-face-recognition/

Los productos de reconocimiento facial también se están utilizando en el Casino Gran Madrid[87]. El sistema consta de tres cámaras Axis con capacidades especialmente diseñadas para el reconocimiento facial, que utilizan la tecnología de amplio rango dinámico (WDR) que permite la identificación incluso en condiciones de contraluz o cuando hay fuentes de luz brillantes a la vista. Este sistema de reconocimiento facial basado en un servidor está totalmente integrado a la configuración de videovigilancia del casino. Desde el centro de control, proporciona una visión facial directa de los últimos individuos que han accedido al establecimiento, así como la posibilidad de realizar búsquedas rápidas, etc.

Herta Security tiene contactos con instituciones internacionales en Europa, y ha coordinado un proyecto financiado por la UE llamado AWARE, que analiza el comportamiento de las multitudes[88] y puede integrarse en cualquier tipo de cámara.

Gracias a este proyecto, Herta recibió en mayo de 2020 el certificado del **Sello de Excelencia COVID-19** de la Comisión Europea[89].

Thales SA es una empresa tecnológica con sede en Francia que ofrece servicios en tres áreas: Aeroespacial, Transporte y Defensa y Seguridad. **FRP**[90] es el sistema biométrico de reconocimiento facial más avanzado de Thales. Se trata de un algoritmo basado en redes neuronales profundas para la detección, el seguimiento y el reconocimiento de rostros. Thales suministra esta tecnología de reconocimiento facial al aeropuerto de Madrid en asociación con **IECISA** y **Gunnebo**[91]. El sistema de reconocimiento facial se ha instalado en las puertas de embarque J40 y J58 de la terminal 4 del aeropuerto.

En septiembre de 2019, Thales en colaboración con **Gunnebo**, una empresa sueca especializada en soluciones tecnológicas de seguridad, han sido seleccionados para llevar a cabo un proyecto en los territorios españoles de Norte de África (Ceuta y Melilla). Han establecido un sistema de control de entrada mediante tecnología de reconocimiento facial, en el que se ha instalado un total de 35 cámaras entre los puntos de entrada y salida de cada una de las fronteras de Ceuta y Melilla, y la plataforma de software de Thales **LFIS** (Live Face Identification System) para el control del sistema de CCTV.

87 Herta Security website. Case Study. 'Casino in Madrid'. Accessed 20/10/2020: http://hertasecurity.com/wp-content/uploads/Case-Study-Casino.pdf

88 European Commission. Horizon 2020 projects. 2019.'Advanced Face Recognition and CroWd Behavior Analysis for Next GeneRation VidEo Surveillance'. Online: http://cordis.europa.eu/project/id/876945

89 S. Stolton (June 2020) 'Crowd monitoring facial recognition tech awarded Commission seal of excellence'. *Euractiv*. Online: www.euractiv.com/section/digital/news/crowd-monitoring-facial-recognition-tech-awarded-commission-seal-of-excellence/

90 Thales Group website. Thales Facial Recognition Technology. Online: www.thalesgroup.com/sites/default/files/database/document/2020-10/gov-unidad-facial-FRP-es.pdf

91 Iberia. 'Lanza una aplicación para el reconocimiento facial en el aeropuerto de Madrid'. Online: grupo.iberia.es/pressrelease/details/109/11818

Xiptic Solucions es otra de las empresas involucradas. Tiene su sede en Vilassar de Dalt, cerca de Barcelona, y está especializada en el control de accesos y comprobación de la presencia física de las personas a través de las nuevas tecnologías.

Desde 2012, el instituto público Enric Borrás situado en Badalona (Barcelona) ha estado utilizando "un sistema de reconocimiento facial y envío de SMS a las familias para controlar la asistencia de los alumnos", tal y como aparece en la Guía de Información Educativa de Badalona para el curso 2019-2020[92].

La compañía Veridas, con sede en Navarra, fue fundada en 2017 como una empresa conjunta entre el Banco BBVA y das-Nano (proveedor tecnológico de la industria de impresión de alta seguridad). Son expertos en Verificación Digital de Identidad y han desarrollado tecnología para la biometría facial, biometría de voz y verificación de documentos de identidad. Además, ha desarrollado para el banco español BBVA una tecnología de reconocimiento facial que permite a sus clientes pagar tras ser reconocidos por una solución biométrica. El banco ha puesto en marcha un proyecto piloto en Madrid que utiliza el reconocimiento facial basado en la biometría para permitir a los empleados realizar pagos sin tener que utilizar ni una tarjeta de crédito ni un smartphone. Los clientes tienen que situarse frente a una cabina con una cámara que reconoce su rostro -previamente registrado en la aplicación- y el pago se realiza automáticamente[93].

Bee the data es una startup que comenzó a operar en 2015 y tiene su sede en Barcelona[94]. Ha estado desarrollando un software a través de cámaras de Inteligencia Artificial y algoritmos que capturan, analizan y comprenden el comportamiento humano en áreas físicas. En la página web del proyecto aparece que la compañía fue premiada con una mención de honor por las agencias de la ley[95]. La empresa está comercializando dos productos:

Beehavior, una solución que emplea algoritmos de aprendizaje profundo de última generación para capturar, analizar y comprender el comportamiento humano en puntos físicos a partir de la alimentación de las cámaras, y se utiliza con fines empresariales.

Beeye, una tecnología de reconocimiento facial masivo, capaz de detectar las características físicas únicas de las personas y utilizada con fines de seguridad.

92 A. Asenjo (2019) 'Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco.' Business Insider, 19 September. www.businessinsider.es/instituto-catalan-usa-reconocimiento-facial-asistencia-484683

93 Das-Nano. Veridas: the Spanish startup that's revolutionizing biomètrics.

94 Infocif. Company profile. www.infocif.es/ficha-empresa/bee-the-data-sl

95 Lanzadera. 'Bee the Data'. lanzadera.es/proyecto/bee-the-data/

FacePhi Biometria es una empresa tecnológica con sede en Alicante[96]. En abril de 2016, FacePhi presentó el proyecto FACCESS a través del programa Horizonte 2020, el mayor programa europeo para la financiación de proyectos de investigación e innovación.

El proyecto FACCESS supone la expansión de la actividad de FacePhi en la Unión Europea mediante la implementación de pilotos de reconocimiento facial en las más prestigiosas instituciones financieras de toda Europa[97].

La Comisión Europea firmó el contrato para el desarrollo y la ejecución del proyecto FACCESS, aprobando así la subvención de fondos perdidos que otorga a la empresa 1,69 millones de euros a desembolsar durante los dos años del proyecto. El proyecto también recibió el sello de "Excelencia" de la Comunidad Europea con una puntuación de 14,48/15.

A principios de 2019, la empresa firmó uno de sus mayores contratos con la catalana CaixaBank para suministrar su software de reconocimiento facial **SelPhi**[98].

Anyvision[99] es una empresa israelí fundada en 2015 por personal académico y expertos en ciberseguridad y especializada en el sector de la tecnología de ciberseguridad y reconocimiento facial. Destacan sus sistemas **Better Tomorrow**, **SesaMe**, e **Insight**. Estos sistemas se utilizan en contextos de seguridad interna, como los controles fronterizos, los aeropuertos y por varias agencias policiales.

Mercadona, una de las mayores cadenas de supermercados de España, ha anunciado la instalación de lo que se supone es un sistema de reconocimiento facial Anyvision, creado para detectar a personas con una condena y una medida cautelar con orden de alejamiento dictada por un juzgado para prohibirles la entrada al establecimiento[100]. La compañía española ha instalado este sistema en unos 40 supermercados de Mallorca, Zaragoza y Valencia[101].

96 Infocif. Company profile. www.infocif.es/ficha-empresa/facephi-biometria-sa

97 FacePh (2016) 'FacePhi beneficiario del mayor Programa Europeo de financiación de proyectos de investigación e innovación'. www.facephi.com/es/noticias/sala-prensa/facephi-beneficiario-del-mayor-programa-europeo-de-financiacion-de-proyectos-de-investigacion-e-innovacion-1/

98 J. Mira (2019) 'Entrevista a FacePhi'. *Estrategias de inversión,* 18 September. www.estrategiasdeinversion.com/analisis/bolsa-y-mercados/el-experto-opina/el-acuerdo-de-caixabank-es-uno-de-los-factores-n-431673

99 Anyvision Profile by ODHE. www.odhe.cat/es/anyvision/

100 E. Pérez (2020) 'Mercadona instala un sistema de reconocimiento facial en sus supermercados'. *Xataka*, 2 July. www.xataka.com/privacidad/mercadona-instala-sistema-reconocimiento-facial-sus-supermercados-como-funciona-que-genera-importantes-dudas-privacidad

101 V. Romero (2020) ' La tecnológica israelí con un asesor exMossad que 'caza' ladrones en Mercadona'. *El Confidencial,* 2 July. www.elconfidencial.com/empresas/2020-07-02/mercadona-reconocimiento-facial-anyvision_2664608/

La empresa israelí Eyesight Technologies es uno de los principales proveedores de sistemas de visión por medio de Inteligencia Artificial instalados en el interior de los vehículos y, junto con el Grupo Antolín, uno de los mayores fabricantes de interiores de vehículos del mundo. Han llegado a un acuerdo de colaboración para ofrecer soluciones de vigilancia de conductores y pasajeros a los fabricantes de automóviles[102]. Eyesight Technologies ha desarrollado el sistema **Cabin Sense** que monitoriza el interior del coche y a los pasajeros permitiendo la personalización y el desarrollo de funciones de seguridad adaptativas. La tecnología de Eyesight Technologies también permite identificar al conductor y detectar acciones como fumar, el uso del cinturón de seguridad o del teléfono móvil.

Grupo Sabico tiene su sede en San Sebastián y está presente en el sector de la seguridad desde 1989. En la Exposición Internacional de Seguridad de 2018 celebrada en Londres, la empresa presentó su sistema de reconocimiento facial, que reconoció muchos de los rostros de los asistentes, incluido el del propio ministro del Interior de la época, a partir de imágenes de su perfil público en las redes sociales.

Según su página web y un vídeo publicado, las cámaras utilizadas para aplicar su software de reconocimiento facial son de **Avigilon**, subsidiaria de **Motorola Corporation**[103]. Sabico también utiliza cámaras Avigilon en el Gran Premio de Aragón de Motociclismo[104].

Desde 2018, a través de un proyecto[105] financiado por el Centro para el Desarrollo Tecnológico Industrial y el Fondo Europeo de Desarrollo Regional, España participa junto a seis empresas del ámbito de la tecnología y la seguridad, entre las que se encuentra la catalana Herta Security, en la implantación de un sistema de vigilancia y control basado en la tecnología 5G y la Inteligencia Artificial, y en la tecnología de reconocimiento facial hasta el punto de desarrollar algoritmos para identificar comportamientos anómalos. Las soluciones resultantes estarán a disposición de las fuerzas del orden y de los agentes de seguridad privada. De hecho, la Guardia Civil ha colaborado con el proyecto, con un presupuesto de 5 millones de euros hasta 2022[106].

102 Eysesight. 'Eyesight Technologies and Grupo Antolin Team Up to Provide Intelligent In-Cabin Monitoring Solutions'. www.eyesight-tech.com/news/eyesight-technologies-grupo-antolin-team-provide-intelligent-cabin-monitoring-solutions/

103 Sabico. 'El reclamo en el Sicur 2018'. www.sabico.com/blog/2018/02/20/sabico-reclamo-sicur-2018/

104 Digital Security. ' Motorland Aragón confía en la tecnología IP de Avigilon para su sistema de almacenamiento CCT'. www.digitalsecuritymagazine.com/2019/04/11/motorland-aragon-confia-tecnologia-ip-avigilon-para-sistema-almacenamiento-cctv/

105 Instituto Tecnológico de Castilla y León. Artificial Intelligence system for Monitoring, Alert and Response for Security in events. www.itcl.es/proyectos-eia/aimars/

106 Orovio (2020) La mascarilla no protege (de la videovigilancia). *La Vanguardia,* 6 September. www.lavanguardia.com/vida/20200906/483329209528/camaras-videovigilancia-interior.html

El proyecto AI MARS facilita la adopción de soluciones tecnológicas para proporcionar información inmediata a las fuerzas y cuerpos de seguridad públicos y privados, así como a los gestores de grandes espacios públicos (centros comerciales, estadios deportivos, etc.) para prevenir atentados, aglomeraciones, disturbios y otros incidentes en grandes concentraciones de personas y otras situaciones con altos requerimientos de seguridad. Esta tecnología, según explica uno de los participantes en el proyecto en la página web de la empresa, también es aplicable al control de fronteras o a la protección de infraestructuras críticas[107].

Otra forma de entrar en el mercado europeo son los clusters tecnológicos y las *Joint Ventures* (alianzas comerciales). Como se ha descrito anteriormente, el "Payment Innovation Hub" de Barcelona es una *joint venture* de CaixaBank, Global Payments, Visa, Samsung y Arval para desarrollar proyectos de I+D. Han ideado un sistema para pagar "a través de la cara" y obtener dinero de los cajeros automáticos después de ser comprobados biométricamente[108]. Lanzadera es una iniciativa de Juan Roig, propietario de Mercadona, ubicada en la Marina de Valencia, que tiene como misión la formación, asesoramiento y financiación de emprendedores. Entre las *startups* financiadas por Lanzadera hay varias que están trabajando con IA para desarrollar tecnología de reconocimiento facial.

107 Instituto Tecnológico de Castilla y León. Artificial Intelligence system for Monitoring, Alert and Response for Security in events. www.itcl.es/proyectos-eia/aimars/

108 R. Sampedro (2020) 'CaixaBank multiplica los cajeros que reconocen caras'. *Expansion*, 6 June. www.expansion.com/empresas/banca/2020/06/06/5edb9581e5fdea6b3b8b45bd.html

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

Reconocimiento facial contra activistas

Las repercusiones de la tecnología de reconocimiento facial y otros sistemas biométricos en los derechos políticos aún no se han determinado por completo, ya que su uso generalizado en la seguridad pública es relativamente reciente. Hasta ahora se sabe que -en manos de las fuerzas de seguridad del Estado- se han utilizado para recoger imágenes en las protestas políticas con el fin de identificar a los manifestantes y cotejar los rostros de los activistas con las bases de datos de delincuentes y terroristas o para aportar imágenes como prueba en los juicios.

A pesar de que la justificación para recoger imágenes de manifestantes en protestas políticas es la comisión de actos criminales, en Cataluña, el País Vasco[109] y otras partes de España[110] se registran a los activistas antes de que se celebren las concentraciones o incluso manifestaciones pacíficas. Alerta Solidària, vinculada a la izquierda independentista catalana y a otras organizaciones anti-represivas, ha denunciado que la policía autonómica de Cataluña realiza "identificaciones preventivas ilegales" a quienes intentan asistir a protestas como la celebración de la Diada Nacional Catalana, exigiéndoles el carnet de identidad y grabando los rostros y las prendas de vestir con cámaras de mano[111].

El **T-Systems** comercializada por la *startup* **Bee the Data S.L.** [112], es una aplicación que permite comparar y buscar coincidencias entre las imágenes tomadas y las bases de datos de delincuentes reincidentes o terroristas buscados internacionalmente. Según los medios de comunicación, la policía catalana decidió hacerse con la aplicación de reconocimiento facial de Bee the Data S.L., pero no la adquirió mediante concurso público sino a través de un contrato marco con T-Systems, por valor de 500.000 euros.

A pesar de la falta de neutralidad y credibilidad general de esta fuente, la plataforma de apoyo a la *startup* Lanzadera también reconoció en su página web que las fuerzas policiales del Estado adquirieron el software de reconocimiento facial Bee the Data en 2017 y que, en 2018, las fuerzas de seguridad le otorgaron una mención honorífica[113].

109 Asociación anadaluza de criminalistas y forenses (2011) 'La captación de la imagen de lugares y personas como medio de investigación penal'. www.aacf.es/2020/07/11/la-captacion-de-la-imagen-de-lugares-y-personas-como-medio-de-investigacion-penal/

110 A. Peláez (2014) 'La Policía graba la protesta contra la 'Ley Mordaza' e identifica a una decena manifestantes '. Diario Sur, 20 December. www.diariosur.es/malaga-capital/201412/20/policia-graba-protesta-contra-20141220223012.html?ref=https:%2F%2F

111 N. Segura Insa (2020) 'Alerta Solidària denuncia 'identificacions illegals' dels Mossos d'Esquadra'. El Nacional, 11 September. elnacional.cat/ca/politica/alerta-solidaria-denuncia-identificacions-illegals-mossos-esquadra_537528_102.html

112 M.A. Ruiz Coll (2019) ' Los Mossos identifican a los manifestantes con una aplicación pagada por la empresa que montó el 1-O'. OK Diario, 1 December. okdiario.com/investigacion/mossos-identifican-manifestantes-aplicacion-pagada-empresa-que-monto-1-o-4857117

113 Lanzadera Company Profile. lanzadera.es/proyecto/bee-the-data/

En varios casos, estas imágenes han sido utilizadas posteriormente en juicios políticos, en los que rasgos como la forma de las orejas o el contorno de los ojos se convirtieron en pruebas para acusar a los activistas. Como argumenta Laia Serra, abogada especializada en derechos humanos y fundamentales, el uso de estas cámaras nunca es bidireccional, ya que *"las imágenes proporcionadas como prueba concluyente de la presencia de un activista en una protesta no pesan lo mismo para identificar a un agente que comete un abuso de poder o una agresión"* en un territorio, incluso aun cuando el uso de pelotas de goma ha provocado la pérdida de un globo ocular en más de 15 ocasiones. En la gran mayoría de los casos en los que se han aportado imágenes tomadas por la policía o por fotoperiodistas para identificar al agente culpable de esta grave violación, han sido rechazadas como prueba definitiva.

"Existe una total falta de control por parte de los ciudadanos y de los defensores de los derechos sobre el uso que se hace de las imágenes que se recogen masivamente en las protestas políticas, en muchos casos con tecnologías de última generación. También hay una falta de control sobre cómo se almacena, se comparte o se destruye esta información o qué tipo de bases de datos se alimentan", confirma la abogada a los autores de este informe.

Este tipo de colección de imágenes de activistas no sólo se está produciendo en las protestas violentas, sino que se está extendiendo a todo tipo de actos políticos. *"He sido testigo de cómo se filma a personas que asisten a desahucios y desalojos sin ninguna infracción, se les graba por ejercer sus derechos políticos. Nadie explica nunca cuál es el uso y el destino de estas imágenes"*, afirma Serra. *"En los expedientes judiciales no se especifica el uso de programas de reconocimiento facial, pero sospechamos que se utilizan porque cuando son arrestados decenas de activistas tras una protesta se les muestra una gran cantidad de fotografías, y es imposible que la policía haya procesado esas imágenes manualmente"*, afirma Eduardo Cáliz, abogado de los movimientos sociales.

Recogida ilegal de ADN

Varios abogados y activistas recuerdan que, en el momento álgido de las recientes protestas políticas en Cataluña, la policía autonómica admitió en algunos juicios que había robado objetos personales -como cepillos de dientes- a las personas desalojadas, con el fin de extraer su ADN. Esta práctica se diluyó, al menos en los casos de protestas y delitos políticos, con la aprobación del GRDP en 2016 y la legislación interna que le siguió. Sin embargo, fue precisamente en 2016 cuando se produjo uno de los casos más claros de procedimiento dudoso en la recogida de ADN de activistas.

En abril de 2016, la policía catalana irrumpió en una conocida casa okupa siguiendo instrucciones de la Audiencia Nacional[114]. Se había tramitado una comisión rogatoria internacional, llevada a cabo bajo el secreto de sumario a petición de la fiscalía de la ciudad alemana de Aquisgrán, que culminó con la detención de una mujer, Lisa. Se trataba de una activista anarquista sobre la que pesaba una orden europea de arresto y entrega por parte de la policía judicial del estado alemán de Renania del Norte-Westfalia, acusada de atracar una oficina bancaria.

El análisis de laboratorio de las muestras genéticas obtenidas a partir de los rastros encontrados en una peluca y otras prendas de vestir, abandonadas en las inmediaciones del banco de Aquisgrán tras el atraco, proporcionó perfiles de ADN a la policía. Estos rastros se enviaron a otros estados europeos para buscar posibles coincidencias en sus bases de datos genéticos. Meses después del suceso, la policía catalana advirtió que había detectado una hipotética coincidencia entre uno de los perfiles genéticos encontrados en la peluca y una entrada -aunque anónima- en su registro. En aquel momento, el uso de esta metodología por parte de la policía en Cataluña para aumentar el control sobre los movimientos sociales era una práctica incierta, pero fue corroborada en cierta medida por el suceso de Aquisgrán y la relación establecida entre estos hechos y la acción política directa en Barcelona en junio de 2009. Los agentes de policía presentes en la manifestación política recogieron pruebas en el lugar de los hechos y encontraron un guante, del que obtuvieron un rastro genético. La muestra permaneció almacenada y sin identificar durante años, hasta que saltó la alarma al cruzarse el rastro con los perfiles obtenidos por la policía alemana en el banco de Aquisgrán[115].

114 ElDiario.es (13 April 20160. 'Los Mossos detienen a una persona en una operación contra un Centro Social de Barcelona'. https://www.eldiario.es/catalunya/persona-detenida-operativo-mossos-blokes_1_4059323.html

115 Solidaritat Rebel. 'Resum Judici'. solidaritatrebel.noblogs.org/post/2017/06/02/breve-resumen-de-la-sesion-23-del-juicio-por-el-caso-aachen-cast/

Dado que necesitaban confirmar la triangulación para incriminar a Lisa, un grupo de policías de paisano siguió a la activista una noche de verano por las calles de Barcelona, recogiendo a escondidas una lata de cerveza vacía que había dejado en la calle. Según los abogados defensores de Lisa, los perfiles genéticos se habían obtenido de forma potencialmente ilegal y sin la autorización de un juez[116], como argumentaron en su juicio en Alemania.

Pero el laboratorio emblemático de recogida de ADN por motivos políticos ha sido históricamente el País Vasco. Especialmente desde el año 2000, con el emergente fenómeno de la violencia callejera o *kale borroka*[117], la policía vasca comenzó a utilizar las pruebas genéticas para acusar a decenas de jóvenes en procesos judiciales, lo que provocó que algunos de ellos sigan cumpliendo penas de prisión excepcionalmente largas[118].

Este hecho condujo al descubrimiento de que la policía regional había estado creando una base de datos desde los años 90 con cientos de huellas dactilares y rastros de ADN recogidos en el lugar de los ataques, para compararlos con otros que a menudo se obtenían sin una orden judicial.

116 Ibid.

117 Estrategia en la confrontación callejera de baja intensidad.

118 Oscar B. de Otlaor (2006) 'ADN contra la kale borroka'. www.diariovasco.com/pg060102/prensa/noticias/Politica/200601/02/DVA-POL-031.html?ref=https%3A%2F%2Fwww.diariovasco.com%2Fpg060102%2Fprensa%2Fnoticias%2FPolitica%2F200601%2F02%2FDVA-POL-031.html

TENDENCIA 5:

RECONOCIMIENTO AUTOMÁTICO DE MATRÍCULAS (RAM)

Ya sea conduciendo, tomando el transporte público o simplemente caminando por la calle, una cosa es segura: estás siendo filmado. En este contexto aparecen las cámaras RAM (Reconocimiento Automático de Matrículas)[119], con tecnología para identificar vehículos. Estas cámaras no se limitan a fotografiar la matrícula, sino todo el vehículo. En España es sólo cuestión de tiempo que cada ocupante del vehículo pueda ser identificado con un módulo adicional de reconocimiento facial.

Las cámaras RAM son capaces de leer las matrículas y de grabar instantáneas perfectamente visibles de los vehículos en marcha (incluso de los que circulan a gran velocidad) gracias a su notable velocidad de obturación, normalmente de 1/10.000[120].

119 Institut Municipal d' Informàtica de l' Ajuntament de Barcelona. 'El nuevo sistema de reconocimiento automático de placas de matrícula de la Guardia Urbana'. ajuntament.barcelona.cat/imi/es/noticia/el-nuevo-sistema-de-reconocimiento-automatico-de-placas-de-matricula-de-la-guardia-urbana_768583

120 M. Merino (2019) Xataka Inteligencia Artificial, 20 August. www.xataka.com/inteligencia-artificial/inteligencia-artificial-tambien-esta-carretera-asi-funciona-reconocimiento-automatico-matriculas-anpr

El sistema se compone de dos lectores de matrículas instalados en el techo del coche patrulla de la policía, cerca de las luces azules de emergencia. Las cámaras graban todas las matrículas que ven a su alrededor. De cada matrícula, el sistema extrae números y letras y los introduce en el equipo informático del coche patrulla para comprobar los datos personales[121].

Pictograma que muestra el funcionamiento del Sistema ATENEA.

EMPRESAS INVOLUCRADAS

Federal Signal es una empresa especializada principalmente en señalización, pero también cuenta con un importante catálogo de productos para las fuerzas policiales. En España la empresa distribuye un sistema llamado **ATENEA**[122] para el control total de los sistemas de señalización, vigilancia, etc. Este sistema facilita el control de todos los dispositivos luminosos y acústicos, las comunicaciones, la gestión y análisis de datos, realiza grabaciones de audio y vídeo, etc. en las condiciones ambientales y de visibilidad más adversas. El sistema ATENEA consta de varias aplicaciones que ayudan a los profesionales de emergencias, entre ellas **FEDRECOGNITION**, el sistema de Reconocimiento Automático de Matrículas (RAM).

En 2019, la empresa proporcionó a la Guardia Urbana de Barcelona 15 pares de cámaras automáticas RAM[123].

121 O. Hernández (2019) 'Cámaras espía de la Urbana pillan 2.400 coches robados en un año en Barcelona'. El Periódico, 23 June. www.elperiodico.com/es/barcelona/20190623/camaras-espia-guardia-urbana-pillan-coches-robados-7518782

122 Sistema Atenea. Online: abuc-system.com/wp-content/uploads/2016/12/P8010003e_Sistema_Atenea.pdf

123 Contractació Pública de la Generalitat de Catalunya. contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCn&idCap=15937468&idDoc=47281108

Omnivision Seguridad[124] es una empresa de seguridad especializada en la realización de fotografías de IA de vehículos que puedan haber cometido una infracción de tráfico. Estas imágenes se comparten con las Fuerzas y Cuerpos de Seguridad. También distribuye sistemas RAM. Uno de sus clientes más importantes es la Guardia Civil[125].

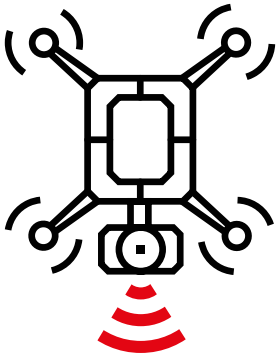
IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

De la misma manera que es cuestión de tiempo que cada ocupante de un vehículo sea también identificado con tecnologías de reconocimiento facial, cabe suponer que la posibilidad de obtener más información sobre los pasajeros va a ser utilizada con fines policiales, no sólo contra las redes delictivas, sino también contra los disidentes políticos. Por el momento, no hay ningún caso documentado.

124 Infocif. Company profile. www.infocif.es/licitaciones/omnivision-seguridad-sl

125 Anuncio de Adjudicación. Contratación del Estado. contrataciondelestado.es/wps/wcm/connect/6065cc94-b284-48d7-8a73-343bc068a54b/DOC_CAN_ADJ2017-584684.pdf?MOD=AJPERES

TENDENCIA 6:



VIGILANCIA CON DRONES[126]

En diciembre de 2017, el Congreso de los Diputados aprobó el Real Decreto 1036/2017, la nueva ley de regulación de drones, dictada por AESA (la Agencia Estatal de Seguridad Aérea), que amplía y concreta el marco legal ante el gran crecimiento de un sector que cuenta con más de 3.000 licencias profesionales en todo el territorio español. Organismos como la Dirección General de Tráfico (DGT), el CNI (Centro Nacional de Inteligencia), las Aduanas y las Fuerzas de Seguridad del Estado quedan exentos del cumplimiento de esta nueva normativa, aunque deben respetar unas normas mínimas.

En un comunicado de prensa emitido en 2018, la DGT dejó clara su voluntad de adquirir drones para el control del tráfico. Este se va a convertir en uno de los mayores mercados para los drones en los próximos años[127].

126 J. Llorca (2020) 'Lo que deberías saber de la vigilancia dron policial que empieza hoy'.VICE, 26 February. www.vice.com/es/article/a34ynk/policia-vigilancia-drones-espana

127 DGT Press Release (2018) www.dgt.es/es/prensa/notas-de-prensa/2018/20180103-accidentes-se-cobran-1200-vidas.shtml

Los drones también se utilizan para controlar a la población en España. Durante el confinamiento provocado por la pandemia del COVID-19, muchas fuerzas de Policía Local utilizaron drones como nueva herramienta de control y vigilancia. Los drones se han utilizado para dar recomendaciones a los ciudadanos, así como para vigilar los desalojos y el acceso a eventos masivos. La policía española fue una de las primeras fuerzas de seguridad del mundo en utilizar drones por control remoto para vigilar a la población.

Los drones fueron utilizados oficialmente por las fuerzas del orden en el Mobile World Congress (MWC) de 2018 por Mossos d'Esquadra, que establecieron el primer dron de vigilancia operativo para garantizar la seguridad pública[128].

La Guardia Civil fue uno de los Fuerzas y Cuerpos de Seguridad del Estado que utilizó drones durante el confinamiento para controlar los movimientos de la población tras las medidas adoptadas durante el Estado de Alarma. En las Islas Canarias, los helicópteros y drones del Servicio Aéreo vigilaban cada tramo de costa para evitar que la gente pudiera trasladarse a su segunda residencia, realizar excursiones a la playa u otras actividades prohibidas como la pesca o la acampada[129].

128 *El Periódico* (2018) 'Los Mossos usarán por primera vez drones para vigilar el Mobile'. *El Periódico,* 22 February. www.elperiodico.com/es/barcelona/20180222/los-mossos-usaran-drones-para-controlar-la-seguridad-del-mobile-world-congress-6642039

129 Press Release Guardia Civil (2020). www.guardiacivil.es/es/prensa/noticias/7323.html

EMPRESAS INVOLUCRADAS

DJI[130] es una empresa privada china y el mayor vendedor mundial de vehículos aéreos no tripulados (UAV, por sus siglas en inglés). La empresa controla dos tercios del mercado mundial, y está especializada en vehículos aéreos no tripulados civiles y en tecnología de imágenes aéreas.

El distribuidor oficial de DJI en España, DJI Ars Madrid, proporcionó a la Unidad Militar de Emergencias (UME) dos unidades de su dron Agras para la fumigación en la lucha contra el COVID-19[131].

En enero de 2020, el Ministerio de Defensa confirmó que España no opera ninguno de los drones de DJI tras ser preguntado por *El País*[132].

Grupo Paukner Durante 40 años A. PAUKNER. S.A. ha suministrado equipos y servicios para drones a los sectores de Seguridad y Defensa en España.

Antes del Estado de Alarma, en abril de 2017, la Guardia Civil adjudicó a la empresa de drones Grupo Paukner un contrato para adquirir un dron táctico. Esta pequeña aeronave no pilotada, según los especialistas, es capaz de realizar grabaciones de "muy alta calidad" a gran distancia[133].

La empresa china **GDU Tech**, a través de su comercializadora en España Droneless, ha estado ayudando a las fuerzas de seguridas de Barcelona, Madrid, Matadepera, Parets del Vallès o Sabadell[134].

Además de las habituales cámaras de visión que suelen portar los drones y que permiten la vigilancia aérea, el dron GDU SAGA puede llevar un altavoz de 120 decibelios que permite alertar y enviar mensajes en directo a larga distancia. También cuenta con una cámara de Imagen Térmica (IR) que permite tomar la temperatura corporal a distancia.

130 Who Profits company profile. DJI. www.whoprofits.org/company/dji-dajiang-innovation-technology-company/

131 DJI Ars Madrid (2020) 'La UME realiza pruebas con drones para la desinfección de grandes áreas, Operación 'Balmis'. djiarsmadrid.com/en/module/ph_simpleblog/module-ph_simpleblog-single?sb_category=blog-dji-ars-madrid&rewrite=la-ume-realiza-pruebas-con-drones-para-la-desinfeccion-de-grandes-areas-operacion-balmis

132 J. Pérez Colomé (2020) '¿Espías en el aire? EE UU quiere prohibir los drones chinos y en España están por todas partes '. *El País*, 16 January. http://elpais.com/tecnologia/2020/01/15/actualidad/1579084416_847707.html

133 La Voz de Galicia (22 May 2017) 'La Guardia Civil refuerza con un dron los sistemas de grabación a distancia'. www.lavozdegalicia.es/noticia/espana/2017/05/22/guardia-civil-refuerza-dron-sistemas-grabacion-distancia/0003_201705G22P16992.htm

134 Droneless.net. 'Policía contra COVID-19'. www.droneless.net/policia-contra-covid-19/

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

El uso de drones para monitorear las manifestaciones políticas en Cataluña

Al igual que en el caso del reconocimiento facial, la principal amenaza que plantean los drones se deriva de su carácter intrusivo e invasivo si se utilizan para obtener información o imágenes masivas de manera ilegal o no consentida. De nuevo, esto afecta al derecho a la privacidad y, con el aumento del control social y la trazabilidad y vigilancia de los ciudadanos[135], se ha reforzado en el contexto de la pandemia.

La pandemia ha acelerado claramente el uso de drones con características aplicadas a las medidas restrictivas, como el mantenimiento de la llamada distancia de seguridad entre las personas. Prácticamente todos los cuerpos policiales de España, incluidas algunas policías locales, han volado estos aparatos para controlar posibles infracciones y multar a quienes las cometen, sin tener en cuenta la situación y su contexto. Algunos de los drones que se han puesto en marcha, como los de la Policía Municipal de Madrid, contaban incluso con cámaras termográficas[136], capaces de medir la temperatura corporal para detectar a las personas con fiebre, independientemente de que ésta fuera consecuencia del COVID-19 o de otras infecciones más frecuentes.

En el uso de drones como mecanismo de control, sin embargo, la pandemia no ha hecho más que exacerbar una tendencia creciente, que comenzó en 2018 cuando la policía catalana hizo volar drones para controlar el espacio aéreo durante el Mobile World Congress de Barcelona[137]. En octubre de 2019, la policía regional utilizó sus seis drones DJI para controlar las grandes manifestaciones contra la sentencia que condenaba a prisión a los políticos y líderes soberanistas catalanes. Estas aeronaves proporcionan imágenes complementarias a las tomadas por los helicópteros policiales, que también están equipados con cámaras de alta resolución. Las imágenes se envían al centro de mando que toma las decisiones.

Un caso en el que se utilizó más claramente esta tecnología con aplicación a la seguridad pública y al control de la disidencia política fue en el partido Barça-Madrid en octubre de 2019 en el Camp Nou, donde un dron capturó imágenes de la protesta organizada por un movimiento de resistencia pacífica llamado Tsunami Democràtic [138].

135 Revista Idees. May 2020. 'Intel·ligència artificial en temps de pandèmia. Punts dèbils i oportunitats de la COVID-19'. revistaidees.cat/intelligencia-artificial-en-temps-de-pandemia/

136 R. Peco (2020) 'Los drones ya se usan para vigilar el distanciamiento y detectar contagios'. *La Vanguardia*, 29 April. www.lavanguardia.com/tecnologia/20200429/48792715052/drones-vigilar-distanciamiento-detectar-contagiados-covid-19-pandemia.html

137 A. Punsí (2019) 'Més vigilants al cel'. *Cadena Ser,* 23 December. cadenaser.com/emisora/2019/12/23/sercat/1577092592_277484.html

138 J. Subirana (2019) 'Los Mossos utilizan drones para vigilar el Barça-Madrid'. *Metropoli Abierta*, 18 December. www.metropoliabierta.com/el-pulso-de-la-ciudad/drones-sobrevuelan-vigilar-barca-madrid_22452_102.html

TENDENCIA 7:

programas informáticos de
PREDICCIÓN DEL DELITO

Una de las prioridades de las fuerzas de seguridad es anticiparse a posibles actos delictivos con el objetivo de mantener el orden a nivel local y nacional. Esta tarea ha recaído históricamente en los analistas, sin embargo, desde finales de los años 90 y con el desarrollo del Big Data y la IA, las fuerzas de seguridad han comenzado a desarrollar programas y métodos informáticos capaces de predecir las circunstancias de comisión de un determinado delito[139].

El término técnico es vigilancia policial predictiva, o análisis predictivo, "el uso de técnicas de análisis, en particular técnicas cuantitativas, para identificar objetivos potenciales que requieran la intervención de la policía, así como para prevenir delitos o resolver delitos pasados mediante previsiones estadísticas", y se basa en el principio de repetición, según la idea de que los delincuentes penales tienden a desarrollar un comportamiento repetitivo cuando su método delictivo funciona.

139 V.Cinelli (2019) 'Prevención del crimen y predicción de delitos: ¿en qué punto está España?'. *Real Instituto Elcano*, 26 June. blog realinstitutoelcano.org/prevencion-del-crimen-y-prediccion-de-delitos-en-que-punto-esta-espana/

EMPRESAS INVOLUCRADAS

EuroCop Security Systems[140] es una empresa de ingeniería, desarrollo, integración y mantenimiento de sistemas informáticos que proporciona apoyo tecnológico a las fuerzas de seguridad y a las empresas relacionadas con la seguridad.

La empresa tiene una fuerte relación con diversos municipios, obteniendo muchos contratos en los últimos años[141]. Una de sus líneas de negocio es el suministro e instalación de sistemas de vigilancia por video con lectura de matrículas totalmente integrados con el sistema propio de la policía local.

Eurocop ha desarrollado un sistema de predicción y prevención de la delincuencia denominado **EuroCop Pred-Crime**. Se trata de un sistema integrado que procesa datos masivos relacionados con el crimen y los delitos menores, basado en un modelo espacio-tiempo e información geográfica de los mapas de calor, y que utiliza modelos matemáticos y algoritmos para permitir la predicción y prevención de delitos.

Bismart[142] es una empresa de consultoría en gestión y análisis de datos. La compañía ha desarrollado una herramienta llamada **Crime Prediction**, una nueva solución para las ciudades inteligentes a la prevención y detección de drogas. La tecnología hace uso de modelos analíticos predictivos y de sensores a través de un área tras monitorizar datos continuos durante un largo periodo de tiempo[143].

Según Albert Isern, director general de Bismart, *"los avances en el análisis de datos y el aprendizaje automático permiten ahora analizar silos de datos, lo que ayuda a los departamentos a identificar no sólo dónde es probable que se produzca la delincuencia, sino también cuándo y en qué circunstancias"* [144].

Como se ha mencionado anteriormente, el programa Horizonte 2020 financia el tipo de tecnología que representa el proyecto europeo Ecosistema profundo de aplicación de la ley RA - **DARLENE** (Deep AR Law Enforcement Ecosystem)[145].

Este proyecto, financiado por la UE, tiene como objetivo ofrecer a las fuerzas del orden europeas un método de seguridad proactiva que les permita analizar volúmenes masivos de datos para predecir, anticipar y prevenir actividades delictivas. Para lograrlo, el proyecto combinará las capacidades de la realidad aumentada (RA) con potentes algoritmos de aprendizaje automático, técnicas

140 Eurocop PRED Crime. 'Análisis y predicción del delito'. www.eurocop.com/sistemas-de-eurocop/analisis-y-prediccion-del-delito/

141 Infocif. Company's profile. www.infocif.es/licitaciones/eurocop-security-systems-sl

142 Bismart. Crime Prediction Software. bismart.com/es/soluciones-business-intelligence/crime-prediction/

143 Muy Computer Pro. 'Bismart desarrolla 'Crime Prediction' para combatir el tráfico ilícito de drogas'. www.muycomputerpro.com/2017/07/18/bismart-crime-prediction-drogas

144 *La Vanguardia* (2017) 'Empresa catalana desarrolla una tecnología para dectectar puntos venta droga' *La Vanguardia*, 17 July. www.lavanguardia.com/vida/20170717/424186840698/empresa-catalana-desarrolla-una-tecnologia-para-detectar-puntos-venta-droga.html

145 Horizon 2020. European Project. *Deep AR Law Enforcement Ecosystem*. cordis.europa.eu/project/id/883297.

de fusión de la información de los sensores, reconstrucción en 3D, tecnología vestible y recomendaciones personalizadas en función del contexto.

El proyecto comenzó en septiembre de 2020 y se prolongará hasta agosto de 2023. Hay varios participantes españoles, entre ellos, El Ayuntamiento de Valencia, el Departamento de Seguridad del Gobierno Vasco y el Centre Tecnològic de Telecomunicacions de Catalunya.

VeriPol[146] es un software desarrollado por Miguel Camacho, un inspector de la Policía Nacional, que evalúa la veracidad de las denuncias presentadas ante la Policía Nacional española. Se introdujo en 2018 después de que Miguel Camacho asistiera a un curso de doctorado sobre policía predictiva en la Universidad de California. El programa extrae características útiles de los relatos de las denuncias mediante técnicas de procesamiento del lenguaje natural. Estos datos son procesados por un modelo matemático que estima la probabilidad de que la denuncia sea falsa.

Además, VeriPol extrapola e identifica patrones de comportamiento a partir de los datos, lo que permite a los agentes de la Policía Nacional comprender las características que diferencian las denuncias verdaderas de las falsas. VeriPol está por ahora disponible en unas 240 comisarías de la Policía Nacional.

146 R. Alvárez (2019) 'La inteligencia artificial de la policía que desenmascara denuncias falsas'. *La Vanguardia*, 13 April. www.lavanguardia.com/tecnologia/20190414/461583468024/veripol-policia-nacional-inteligencia-artificial-algoritmo-denuncias-falsas.html

IMPACTO EN LOS MOVIMIENTOS SOCIALES Y OTROS ACTORES POLÍTICOS

Según Sheila Queralt, forense especializada en lenguaje policial y directora de la empresa SQ Forensic Language de Barcelona, las denuncias escaneadas por VeriPol son redactadas por los propios agentes de las comisarías, lo que significa que pasan por un primer filtro antes de ser procesadas por el programa informático. Esto, unido a la forma en que el algoritmo fue entrenado (un agente especializado definió si las alegaciones eran o no falsas), demuestra que *"los parámetros analizados no son objetivos"*[147].

En España, estas tecnologías están siendo desplegadas por cuerpos policiales como la Policía Local de Castellón, que está utilizando una herramienta pionera que permite trasladar a un mapa el riesgo de comisión de un determinado delito[148]. Al basar estos sistemas en datos desnudos sin contexto, además de descuidar la importancia de la prevención, puede conducir a la estigmatización de determinados barrios y a tratarlos como escenarios de delitos, en lugar de trabajar para prevenir las causas estructurales que pueden facilitar la delincuencia. Por otro lado, algunas de las actividades que realizan los grupos políticos disidentes se consideran formalmente delictivas -por ejemplo, en virtud de leyes que limitan abiertamente los derechos y las libertades, como la Ley de Seguridad Ciudadana de 2015-, por lo que las tecnologías de prevención del delito pueden suponer claramente una mayor persecución y acoso a los movimientos sociales.

147 N. Bellio (2020) '*Spanish police plan to extend use of its lie-detector while efficacy is unclear*'. *Algorithm Watch*, 27 October. algorithmwatch.org/en/story/spain-police-veripol/

148 C. Prego (2018) 'Si con la tecnología podemos predecir crímenes la gran pregunta es ¿debemos?'. *Xataka*, 8 September. www.xataka.com/legislacion-y-derechos/tecnologia-podemos-predecir-crimenes-gran-pregunta-debemos

CONCLUSIONES

Es innegable que el poder de las tecnologías de vigilancia masiva y control de la población se ha expandido en las últimas dos décadas bajo la principal justificación de la "lucha contra el terrorismo". A la vez que se han potenciado prácticas como la supervisión de las comunicaciones; el almacenamiento de una gran cantidad de datos de ciudadanos privados; la proliferación de cámaras de videovigilancia con sistemas de reconocimiento cada vez más sofisticados; la localización con sistemas de posicionamiento GPS; la implantación de tecnologías basadas en la huella digital, los rasgos faciales o la lectura del iris; sin embargo, las limitaciones del uso de estas tecnologías invasivas han ido desvaneciéndose al mismo ritmo que dificultan la defensa de los derechos humanos y fundamentales.

El precario equilibrio entre seguridad y libertades gira ahora claramente hacia una normalización de la invasión de todas las parcelas de nuestra intimidad, tendencia que la actual crisis sanitaria ha acelerado.

El concepto de "Ciudades Inteligentes" es otra excusa para aplicar este tipo de tecnologías. El Gobierno español, a través de la iniciativa Red.es[149] y su Agenda Digital, apuesta claramente por la implantación del concepto de *Smart City* en las ciudades españolas, especialmente a través del Plan Nacional de Ciudades Inteligentes, que cuenta con un presupuesto de 188 millones de euros.

Incluso Cataluña tiene su propia estrategia de ciudad inteligente, *Smart Catalonia*[150], que está en línea con la estrategia *Europa 2020* de la Comisión Europea.

Smart Catalonia pretende convertir a Cataluña en un 'Smart Country' internacional de referencia, utilizando la información y la tecnología digital para aportar innovación a los servicios públicos, impulsar el crecimiento económico y promover una sociedad más inteligente, sostenible e inclusiva.

Barcelona, como capital de Cataluña, ha dado pasos para convertirse en una 'Smart City' ya que ha firmado varios acuerdos con diversas empresas tecnológicas como **Huawei**. En 2019, el Ayuntamiento de Barcelona y Huawei firmaron una Carta de Intención para colaborar en la facilitación de inversiones para proyectos innovadores de nuevas tecnologías en la ciudad. La colaboración se firmó en uno de los mayores "escaparates inteligentes" del mundo, el Smart City Expo World Congress (SCEWC) que tuvo lugar en Barcelona en 2019.

En España, las autoridades locales recopilan enormes volúmenes de datos sobre los ciudadanos y visitantes sin su conocimiento. Hay numerosos ejemplos de esta información que se recoge sin que nadie se dé cuenta: datos de smartphones, sensores de tráfico, cámaras, etc. Estos proyectos de "Ciudades Inteligentes"

149 Red.es it is a public entity attached to the Ministry of Economic Affairs and Digital Transformation through the Secretary of State for Digitalisation and Artificial Intelligence.

150 Smart Catalonia strategy of the Government of Catalonia. smartcatalonia.gencat.cat/en/smartcat/que_es/

también cuentan con el apoyo de la Comisión Europea como parte del Proyecto 4ALLCITIES en el marco del Programa Horizonte 2020: Seguridad de los espacios inteligentes para todas las ciudades[151].

Casi todos los datos que se recogen y utilizan se toman sin ninguna autorización de la ciudadanía. Es muy difícil que alguien dé su permiso sin tener claro qué datos se recogen exactamente, ni la razón para hacerlo. Las autoridades locales mencionan una variedad de propósitos para sus iniciativas de "Ciudades Inteligentes": publicidad, turismo, sostenibilidad, movilidad, desarrollo urbano y seguridad. Sin embargo, no se ha definido claramente el ámbito en el que se utilizará finalmente esta información.

Además, todas las tecnologías que se han descrito en este informe tienen el potencial de interconectarse a los centros de mando y control de la Policía, confiriendo más "poder" a las fuerzas de seguridad y al Estado para controlar a sus ciudadanos.

Este informe identifica una tendencia a la expansión de los sistemas de vigilancia y de las tecnologías de control de movimientos. Se trata de una tendencia que la pandemia del COVID-19 está contribuyendo a normalizar y legitimar, probablemente de forma permanente y sin herramientas de rendición de cuentas que permitan examinar los posibles abusos de poder cometidos por las fuerzas de seguridad del Estado y las empresas que controlan y almacenan todos estos datos.

Como Iridia y Novact, dos organizaciones de la sociedad civil catalana han indicado *"la lucha por el control del COVID-19 está contribuyendo a acelerar el desarrollo de nuevos sistemas de vigilancia biométrica en los espacios públicos. Los datos recogidos se sistematizan en bases de datos que clasifican a las personas asignando los riesgos que ese individuo supone para la sociedad"*[152]. Todas estas medidas, probablemente necesarias a corto plazo, exigen un cambio de dinámica una vez la pandemia esté controlada. La respuesta a largo plazo a esta crisis dependerá de la forma en que las ciudades reaccionen a la obligación de satisfacer necesidades esenciales, pero parcialmente conflictivas: seguridad y libertad, privacidad y acceso a los datos. Los conceptos de Ciudad Inteligente y Ciudad Segura parecen ser una excusa más para el proceso de securitización en curso.

El enorme impacto sanitario, político, social, económico e incluso cultural que el COVID-19 ha generado en nuestras sociedades, podrá ser superado. Sin embargo, está claro que las tecnologías de control social que vinieron con él parecen haber llegado para quedarse.

151 Horizon 2020. European Project. *Smart Spaces Safety and Security for all Cities.* cordis.europa.eu/project/id/883522

152 Irídia and Novact. October 2020. Report: 'Vulneraciones de los derechos humanos en las deportaciones' (p.128). iridia.cat/wpcontent/uploads/2020/11/Deportaciones_FinalMOD_Imprimir-2.pdf

Imágenes:

Portada:
Fotomovimiento_Joanna Chichelnitzky,
Diada de Catalunya 2020

Portada interior:
Lucía Armiño

Página 4: Fotomontaje.
Imagen original:
Juan Lupión_Wikipedia Commons

Página actual:
Barcex_Wikipedia Commons,
Manifestación del 12 de mayo de 2012
en Madrid

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