

MASS SURVEILLANCE AND CONTROL OF EUROPEAN DISSIDENCE

SPAIN

High-tech surveillance in times of COVID-19

How digital technologies penetrate public security spheres and impact civil liberties in Spain

Authors: Nora Miralles, Giulia Campisi and Carlos Díaz (ODHE)

Editors: Lina M. González and Felip Daza

Design: Lucia Armiño

Proofreading: Lucy Powell

Published by European Network of Corporate Observatories,

Shoal Collective, Observatory of

Multinationals and Observatory of Human Rights and Business

in the Mediterranean region (Novact and Suds).

Supported by a grant from the Open Society Foundation,

International Catalan Institute for Peace,

and Barcelona City Council.

Contents of the report may be quoted or reproduced for non-commercial purposes, provided that the source of information is properly cited.

Barcelona / April 2021

ACKNOWLEDGEMENTS

We would like to thank everyone who has been willing to speak to us and share their story, even when it is not a pleasant one. We offer special thanks to everyone who has suffered directly from the forms of surveillance we describe.

This report and the webdoc are part of the research, advocacy and education projects coordinated by Suds and Novact in collaboration with Shoal Collective and the Observatoire des Multinationales. The donors are not responsible for any use that may be made of the information it contains.



1

Methodology

2

Introduction

4

Chapter 1:
Legal
framework:
Spain as a
surveillance
state

13

Chapter 2:
Trends

- 14 Government hacking: digital infiltration and spyware
- 19 Audio and image surveillance on public spaces
- 24 Interception of communications and data extraction by law-enforcement agencies
- 34 Facial recognition and biometric technology
- 46 Automatic Number Plate Recognition (ANPR)
- 49 Drones surveillance
- 53 Crime predictions software

57

Conclusions





METHODOLOGY

Our research presents an overview of mass surveillance in Spain with a focus on the use of technology against activists, certain communities or groups and other political actors. It is based on the following research methods:

- Review of corporate profiles on professional company databases, the industry press, and information made available by journalists, researchers and campaign groups.
 - Search of the EU Tenders Electronic Daily website, the Spanish Tender website, and the Regional and Local Tender websites.
 - Search for contracts awarded by the government and law-enforcement agencies.
 - Interviews with campaigners, activists, lawyers, experts and other members of the public who are affected by the technology.
- 
- 



INTRODUCTION



In recent times, two trends have converged that have greatly contributed to expanding the Spanish government's digital agenda and normalising technologies that can be used for mass surveillance. These processes are also aligned with the trend of curtailing rights and freedoms in the name of national security and narrowing the political space for citizens, facilitating the use of these technologies to monitor dissident political groups.

On the one hand, the development of cities into 'Smart Cities' is one of the solutions being given to the unstoppable growth of urbanisation and the many challenges it presents in terms of public security. According to the United Nations, 55% of the world's population currently resides in urban areas. It is expected to increase to 68% by 2050. **This growth has led to the thinking of solutions to alleviate the potential problems of over population and how to control it.**

The Smart City then becomes a complex system involving different agents. Hundreds of thousands of sensors are counted within this system that measure various things, such as pollution, vehicle registration plates, and people.

In this sense, surveillance and control technologies play a key role in the system of a Smart City. Historically, the concept of Citizen Security has been one of the great aspirations and excuses in justifying the application of restrictive measures. Now, under this concept, surveillance and control technology has been installed everywhere with the aim of combating crime, but at the same time always having access to observe and analyze everything that happens in the city.

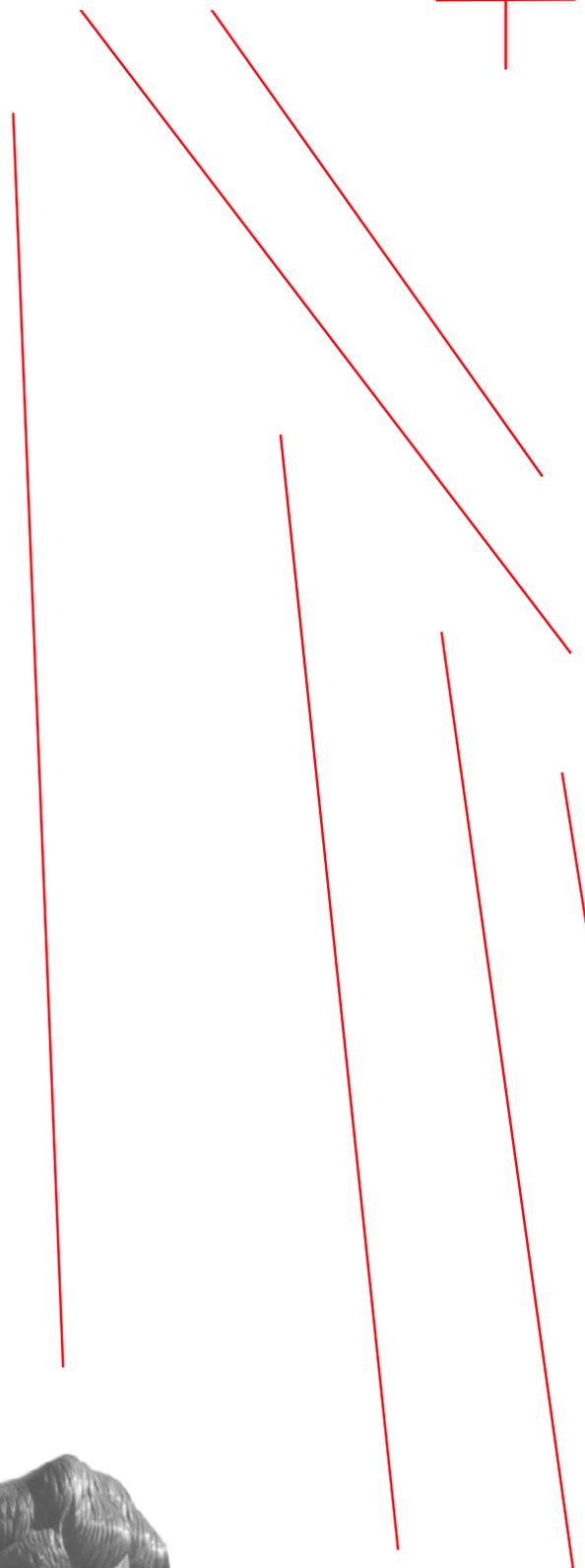
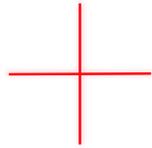
On the other hand, these potentially mass surveillance activities are reinforced by the relationship between corporations and government agencies. With the rise of neoliberal ideology at the end of the last century, the relationship between public agencies and the private sector became stronger. This relationship is crucial to understand the phenomenon of mass surveillance, not only because it is private sector companies that provide knowledge and technology, but also because the data that government agencies need for population control in many cases originates from internet searches, social media interactions and phone calls, making the **relationship between public institutions and cybersecurity and tech companies indispensable.**

The advent of COVID-19 appears to be underpinning this trend for public-private partnership, with government and business joining forces to exert a new form of social control in the name of health and public security, using technology to transform private life into being part of a system of domination.

Moreover, the pandemic provides a prolific context to expand the uses of systems such as facial recognition or drone surveillance, which could already be impacting privacy and may further hinder the exercise of civil and political rights, as their use in demonstrations and against dissident groups is already a reality.

High-tech surveillance in times of COVID-19

1 LEGAL FRAMEWORK: SPAIN AS A SURVEILLANCE STATE



In recent years, digital development has been pivotal for successive Spanish governments, seeking to make Spain one of the most 'digitised' countries in the European Union (EU). In 2019, the digital economy represented 19% of Spain's gross domestic product (GDP) and the government started designing an Artificial Intelligence Strategy and an ambitious Digital Plan. Little attention has been paid to transparency, citizenship participation and digital and civil rights. The focus on security and technologies in the context of the pandemic has resulted in the deepening of a digital surveillance system.

Before the outbreak of COVID-19, the Spanish government was already taking steps to base part of its security system on mass surveillance, having approved the Royal Decree-Law 14/2019 in October 2019. This law, also known as the digital gag law, allows state agencies – irrespective of judicial authorisation – to intervene in the internet and take control of the digital infrastructure of certain entities.

The Royal Decree-Law 14/2019 has raised concerns in civil society and among non-government organisations (NGOs) such as Amnesty International, which claims that this *"is developed within the framework of a purely administrative procedure, without judicial control, to guarantee the supervision of the process"*.¹ These concerns do not seem to have been taken into account since the same controversial articles in the Decree-Law also appear in the draft of the new Telecommunications Law.

Another legislative measure is the Resolution of the Secretary of the Presidency, Relations with the Courts and Democratic Memory, approved in July 2020, which allows law enforcement agencies (LEAs) to install facial recognition systems at access points for mass events, as well as a mobile phone detection system based on IMSI-catcher technology, with the aim of "providing alerts to security officers in order to detain people who have pending cases with the Justice system".

In July 2020 the Spanish government presented its digital agenda 'España Digital 2025'. One of its objectives is to "move towards a data economy, guaranteeing security and privacy and taking advantage of the opportunities offered by Artificial Intelligence with the aim that at least 25% of companies use Artificial Intelligence and Big Data within five years", and strengthen Spanish cyber security.²

1 Amnesty International (2020) 'El Real Decreto Digital propicia la censura previa y el secuestro de contenidos en internet'. Online at: 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. www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf

In early November 2020, the Spanish government approved the Order PCM/1030/2020,³ where the National Security Council establishes a protocol to act against fake news. This initiative is inspired by the EU European Democracy Action Plan and the 2018 EU Action Plan on Disinformation, created to avoid interference in democratic elections and the publication of disinformation about them. Nevertheless, this Order could represent an attack on freedom of expression, a fundamental right enshrined in the Spanish constitution, since the core measure of the protocol is the continuous monitoring of networks. To comply with this national plan, the government has created a structure involving the National Security Council, the Situation Committee, the Secretariat of State for Communication, the Standing Commission against Disinformation and the competent public authorities, including the Presidency, ministry communication cabinets and the National Intelligence Centre (CNI), which clearly demonstrates a securitisation of the information. The Order envisages the possibility of involving private-sector actors, which play a fundamental role *“in the fight against the disinformation, with actions as identification and no contribution to its diffusion [...] and developing tools to stop the spread of [disinformation] in the digital environment.”* The Order does not state clearly why and how private actors will be involved in the decision-making process in the fight against disinformation, which has already raised concerns about the independence and freedom of information.

Meanwhile a new EU Digital Service Act is about to be approved and will give European guidelines to all member states for approaching this kind of policy. Although the Act has not yet been approved at the time of writing, the Resolution approved by the European Parliament on October 2020, referring to the EU Commission on the future Digital Service Act, Resolution on the Digital Services Act and fundamental rights issues (2020/2022(INI)),⁴ contains recommendations and considerations of this kind: *“whereas a pure self-regulatory approach of platforms does not provide adequate transparency, accountability and oversight; whereas such an approach neither provides proper information to public authorities, civil society and users on how platforms address illegal content and activities and content that violates their terms and conditions, nor on how they curate content in general”*; and *“whereas such an approach may not guarantee compliance with fundamental rights and creates a situation where judicial responsibilities are partially handed over to private parties, which poses the risk of interference with the right to freedom of expression.”* This means that both Spanish government initiatives could be seen as a threat to the right to freedom of expression, due to the important role given to private-sector actors to determine what kind of content constitutes hate speech, and perhaps decide and campaign on what is disinformation or information.

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

Another important point is that the EU General Data Protection Regulation (GDPR),⁵ established in 2016, regulates all treatment of personal data in all member states. The EU Regulation aims to protect personal information, guaranteeing this fundamental right proclaimed in Article 8 of the Charter of Fundamental Rights of the European Union.⁶ Concerning the type of data that has to be protected, the Regulation lists biometric data, defined as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.” This is the kind of data processed by surveillance tools and technology such as facial recognition. Article 9 of the GDPR states that: *“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”* Subsequent paragraphs establish exceptions to this prohibition, allowing the processing of specific data in certain cases such as where people give their consent, where they are unable to give explicit consent due to health reasons, and where: *“g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respecting the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.”*

Spain adapted the EU Regulation in the Organic Law 3/2018, on Protection of Personal Data and guarantee of digital rights,⁷ in December 2018, but there is as yet no sign of any regulation on biometric data. Nevertheless, there are some articles dedicated to the regulation of data obtained through the use of cameras, stating that their use is permitted when necessary, to safeguard public security. There is clear evidence that the pretext of acting in the public interest or national security has been increasingly used – and abused – to allow mass surveillance, that, in effect, permits the securitisation of society.

While trying to regulate the domestic digital environment, the EU seems to have been ‘exporting’ tools, training and skills in digital surveillance to non-EU members, mostly to Eastern Europe and countries in West Asia and North Africa, through various EU cooperation funds and agencies, particularly police cooperation agencies, such as the European Union Agency for Law Enforcement Training (CEPOL). Privacy International obtained access to several documents that show

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

evidence that this is happening,⁸ Among the several documents and sources obtained by Privacy International, two projects that deserve attention are, one in Senegal, which aims to create a national biometric database to “address the root causes of irregular migration funded through the EU Trust Fund for Stability and Addressing Root Causes of Irregular Migration and Displaced Persons in Africa⁹”, Such examples show European expertise in digital surveillance being exported, along with the concept of securitisation of migration.¹⁰

The Spanish government contributes to many of these projects and programmes indirectly through EU agencies (mostly in the field of migration and border management in the Maghreb) and directly through institutions as the Policía Nacional, which has been directly involved in providing training sessions on digital surveillance skills and technologies, as Privacy International discovered.

In Bosnia and Herzegovina, the Policía Nacional provided a training session for local police and intelligence authorities on financial investigations, which “*outlines potential avenues for tracking IP addresses, emails, and conducting wiretapping.*” Furthermore, “*a slide towards the end of the session also promotes the use of malware or computer trojans – software used to hack into devices to extract data and take control of functions such as the camera and microphone – and sold on the open market by companies such as NSO Group,*”¹¹ clearly showing how practices of questionable legality are commonly used and strongly recommended by Law Enforcement Agencies.

There have also been concerns about privacy in relation to the mobile applications developed by some Spanish regions for COVID-19 contact tracing: “*We have found that these applications are very poorly designed from the point of view of respect for privacy. They are very invasive, they claim that they are not necessary to make this coronavirus diagnosis, they share with Google and Facebook, and even with SMEs that have developed the software,*”¹² claims Gemma Galdón, a privacy analyst and Director of Eticas Consulting.

At the same time, military and defence companies, using the pretext of COVID-19, are willing to make deals with surveillance and control technologies. According to an Amnesty International report, companies such as Thales Group are not exercising due diligence in preventing their products from being used in potential human rights violations and even war crimes.¹³ Thales, and its subsidiary Gemalto, are also among the companies that benefit most from the militarisation

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%2011%20Termes%20de%20r%C3%A9f%C3%A9rence%20SN.pdf%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

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/

of European borders.¹⁴ Since 2008, THALES Data Science and Artificial Intelligence Laboratories have been developing a crowd-simulation engine called SE-Star, which makes it possible to manage and observe different variables such as motivational factors and emotions, stimuli, personalities and behaviours in order to control crowd flows.¹⁵ In Spain, Thales has supplied Madrid airport with facial recognition technology using a biometric system called FRP (Face Recognition Platform).¹⁶ These companies are using the pandemic to apply their technology, which also has an impact on civil liberties. Fighting the pandemic has given governments the perfect excuse to exercise their control, surveillance and data collection in partnership with the private sector.

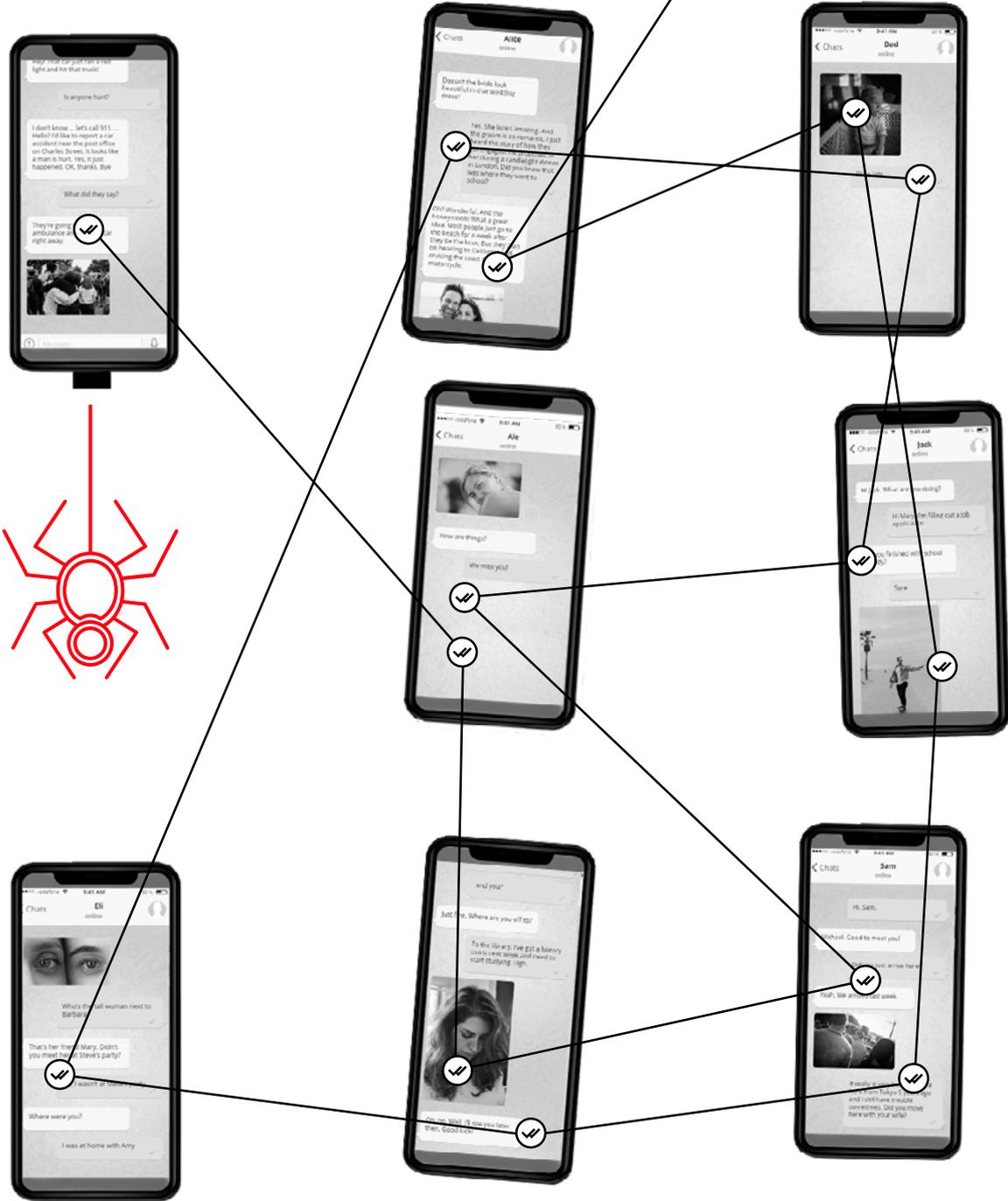
¹⁴ Thales Group website. 'Thales Gemalto EES Border Management System'. www.thalesgroup.com/en/markets/digital-identity-and-security/governmentgovernmentgovernment/EES-border-management-system

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'. www.computing.es/mundo-digital/noticias/1119377046601/frp-solucion-biometrica-de-thales-contener-covid-19.1.html

High-tech surveillance in times of COVID-19

2 TRENDS



TREND 1:

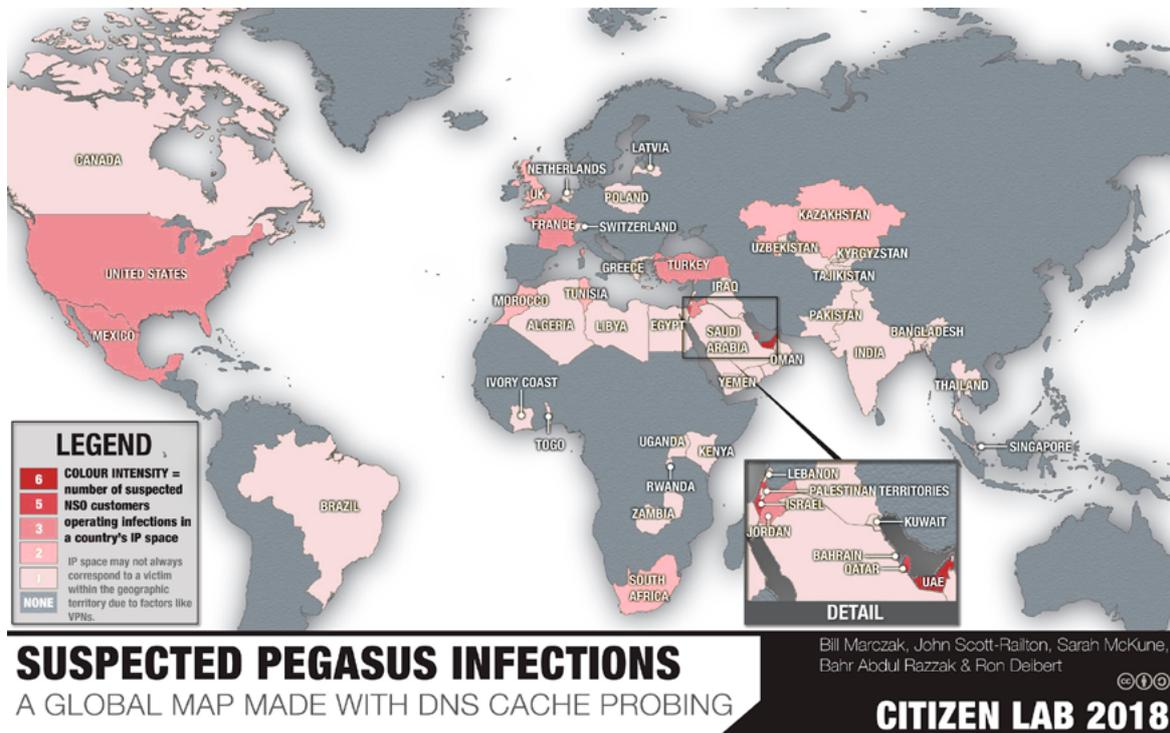


GOVERNMENT HACKING:
digital infiltration
and spyware

In mid-2020, a Citizen Lab investigation exposed the use of **Pegasus spyware** – linked to Israeli company NSO and acquired by Spanish intelligence in 2015 – to spy on the archives, photographs, web-browsing history, emails and other data of Catalan pro-independence politicians. In response to the pandemic, **NSO Group** offered states a new ‘big data’ analysis tool to map the movement of people and their contacts, aimed at helping to curb the virus. Activists and lawyers have recently detected the adaptation of classic techniques such as police infiltration of the digital environment through the use of phishing technologies, mail spoofing and digital infiltration via email and messaging networks such as WhatsApp or Telegram.

COMPANIES INVOLVED

NSO Group is an Israeli cybersecurity company founded in 2010 by Niv Carmi, Omri Lavie and Shalev Hulio, whose executives are believed to have served in Israel's Intelligence Unit 8200.¹⁷ It focuses on creating intrusion and surveillance software such as **Circus** and **Pegasus**, that is later sold to governments, irrespective of the nature of the regime. Unit 8200 is known to use surveillance methods to spy on the Palestinian population.¹⁸ **Pegasus** spyware makes it possible to read messages, access mobile content and even activate mobile components such as the camera or microphone, exploiting critical vulnerabilities to attack mobile phones remotely. According to the Canadian watchdog Citizen Lab, the spyware has been used in at least 45 countries, including Bahrain, United Arab Emirates, and Saudi Arabia.¹⁹



Source: Citizen Lab 2018

17 DW (2020) 'Israeli Spyware threatens to shut down abusers'. 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-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

According to *VICE Magazine*, the Israeli company entered the Spanish market through a 2015 contract with the Spanish government. Motherboard, the Tech section of *VICE*, spoke with a former NSO employee who said: *"We were actually very proud of them as a customer, finally a European state"*.²⁰

Circles is an Israeli surveillance firm that exploits weaknesses in the global mobile phone system to get all personal information and access to calls, texts and location in seconds, simply by knowing the phone number and without hacking the phone itself. According to its employees, it is sold exclusively to governments. Circles is affiliated with the Israeli NSO Group, as a spokesperson told Motherboard: *"NSO and Circles are separate companies within the same corporate family, both of which lead their industries in a commitment to ethical business and adhere to strict laws and regulations in every market in which they operate"*.²¹ Citizen Lab, the Canadian cybersecurity watchdog, has discovered that Circles has been detected in at least 25 countries.²² The company employs a technical system known as **Signalling System 7 (SS7)**, which works when a person travels to another country with their phone and the SS7 network moves the phone to another telecom provider in order to adjust billing. Circles obtains the coordinates of the cell tower closest to the phone and so determines its location and gets into its data and communications.

20 J. Cox & L. Franceschi (2020) 'Source: Spain is Customer of NSO Group', Motherboard Tech by VICE, 14 July. www.vice.com/en/article/pkyzxx/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 CitizenLab (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/

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

Using Pegasus to spy on pro-independence politicians

It is no secret that the Spanish state spied on Catalan politicians and pro-independence activists, as it did on other political groups. But nothing was as controversial as the finding that the security services possessed the **Pegasus**, developed by the Israeli company NSO Group.

In July 2020, Citizen Lab discovered that the mobile phones of several politicians in Spain, including that of the President of the Catalan Parliament, Roger Torrent, were hacked in 2019, along with 100 other figures from civil society around the world.²³ All of them were targeted by Pegasus, in theory sold to governments to fight organised crime and terrorist networks, but instead used by many governments around the world to spy on political opponents and journalists. Torrent's phone would have been infiltrated through a missed WhatsApp call in 2019. He immediately accused the Spanish state of being behind the phone hack, which he believed had probably occurred without a court order.²⁴ This was the first known case of a European state acquiring and using Pegasus against elected politicians.

In addition to Torrent, researchers at Citizen Lab at the University of Toronto Munk School – who collaborated with WhatsApp after the alleged hacking attempts were discovered – alerted two other pro-independence politicians in 2019 that they had been targeted: Ernest Maragall, former Foreign Affairs Councillor and also a Member of Catalan Parliament for the same pro-independence party as Torrent,²⁵ and Anna Gabriel, a former regional MP for the far-left, anti-capitalist Popular Unity Candidature (CUP),²⁶ who is currently living in Switzerland after fleeing Spain to avoid imprisonment for allegedly promoting the 1st October 2017 referendum.

23 S. Kirchgaessner and S. Jones (2020) 'Phone of top Catalan politician 'targeted by government-grade spyware'. *The Guardian*, 13 July. <https://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 espiaats per una empresa que només treballa amb governs'. *El Temps*, 14 July. www.eltamps.cat/article/10826/roger-torrent-i-anna-gabriel-espiaats-per-una-empresa-que-nomes-treballa-per-governos

25 J. Gil (2020) 'El programa espia 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%A9fono-de-anna-gabriel/45902840

Regarding the abuses committed through the use of this spyware, the technological know-how acquired by the company's founders and engineers in Israeli intelligence and defence units has been developed to curtail the civil liberties of Palestinian organisations and activists under surveillance.²⁷ For this reason, several human rights organisations have sought to revoke the company's export license,²⁸ on the basis of the multiple cases of use of this software by states that commit grave violations of human rights.

Mail spoofing and phishing to digitally infiltrate social movements

In October 2020, the grassroots Catalan newspaper La Directa released information concerning the spoofing of at least 11 email accounts of political organisations, youth movements, community meeting places and housing unions.²⁹ According to the activists, more than 60 fake emails were sent with the clear objective of gathering information on the organisations' activities and internal documents, targeting some of the political spaces that currently mobilise people in Spain, such as the pro-independence movement or the housing rights movement. To prevent IP addresses from being unmasked, the users who designed this system used a VPN service, which makes it possible to conceal the identification number and location of the device. However, the journalists who investigated this scandal are certain that several of the IPs detected, point to the Catalan regional police, Mossos d'Esquadra, and to the Centre for Telecommunications and Information Technology of the autonomous government of Catalonia.

"This digital infiltration occurred through the intrusion into personal mail and corporate accounts of political organisations, without any court order or authorisation in case this infiltration actually comes from police forces," explains Eduardo Cáliz, who is part of the legal team acting on behalf of the impersonated activists to get to the heart of the matter.

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/>

TREND 2:



**AUDIO AND IMAGE SURVEILLANCE
ON PUBLIC SPACES**

The use of CCTV technology in public spaces is an established mechanism of control and surveillance in our everyday life. Law Enforcement agencies in Spain rely on video surveillance as a tool to fight crime and monitor population behaviour. According to a report by Comparitech,³⁰ Madrid is among the five EU cities with the highest density of street cameras, with 4.42 camera devices per 1,000 inhabitants. According to Comparitech, only Berlin, London, Vienna and Warsaw have more cameras per person. There are a total of 29,000 security cameras across 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/

COMPANIES INVOLVED

CTRL4 ENVIRO³¹ This Catalan start-up was founded in 2006, arising from a research project and the Universitat Autònoma de Barcelona. The company specialises in means to monitor people's movements, such as monitoring urban flows. COVID-19 has been the impetus to design an entirely new technology that makes it possible to monitor crowds in public spaces such as beaches. Its **MDS** (Social Distance Monitor) is a system capable of anonymously analysing CCTV images in order to control social distancing, the appropriate use of masks and the density of occupation, such as one of Barcelona's most famous beaches.³²

SICE, a subsidiary company of the ACS Group,³³ Sociedad Ibérica de Construcciones Eléctricas, S.A. (SICE) is a multinational technology integrator in the field of traffic and transport, environment and energy, telecommunications and various industrial processes.

One of its key products are surveillance cameras. In 2015, SICE installed 47 new surveillance cameras in central Madrid, ten of which include an innovative analytical software that alerts the police if it detects certain 'strange' behaviours, such as a group of people running, allowing the police to intervene more rapidly.

The images captured by the cameras are distributed through a proprietary fibre optic network that securely attaches the camera to the headquarters of the Municipal Police and the Video Signals Integral Centre (Cisevi). The viewing of this material is restricted to a specifically authorised group in the municipal police, and stored for a maximum of seven days, after which the images are automatically deleted if they are not subpoenaed by the police or a judge.

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

Another operational context where CCTV plays a major role is at the country's borders. In Spain, a handful of companies have been benefiting from the 'border businesses'. In 2013, the Ministry of the Interior awarded a contract for the installation of 42 CCTV devices along nearly 12 kilometres of the fence separating the autonomous city of Melilla from Morocco.³⁴ According to the news agency EFE, sources from the Government Delegation in Melilla advised that the project will be entrusted to **Cobra Instalaciones y Servicios S.A.**, a subsidiary of the **ACS Group**.

In early 2019, the Spanish Council of Ministers approved a Plan of Measures for the Strengthening and Modernisation of the Land Border Protection System in the Autonomous Cities of Ceuta and Melilla. One of the measures is the installation of a new CCTV system on the perimeter of Ceuta, with 66 cameras. The plan also promotes the installation of facial recognition systems at the border posts of El Tarajal (Ceuta) and several locations in Melilla,³⁵ where apparently Gunnebo and Thales are in conversation with the Spanish Ministry of Interior to develop the project.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-enlaceceutaymelilla.aspx

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

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

The expansion of CCTV in city centres as a public security measure for preventing crime coincides with the gentrification of some of these areas and that these are also where mass demonstrations tend to take place. The use of increasingly sophisticated vision and behavioural detection and analysis systems in these CCTV devices located in public areas means the increasing encroachment on civil liberties such as the right to privacy and mobility.

The increase in social control in public areas with CCTV also coincides with the deployment of CCTV in neighbourhoods with a high incidence of drug trafficking, theft and other criminal activities, such as Lavapiés – where 48 CCTV cameras were installed to monitor the entire area from Tirso de Molina Square to the Glorieta de Embajadores – at the heart of political mobilisation³⁷ – and Vallecas in Madrid. Both of them are also very politically mobilised neighbourhoods where, for example, there are strong movements against evictions, organised migrant groups and anti-fascism, and where police operations are periodically carried out against political dissidents and migrants. In this way, such technology can be used not only to deter criminal activity, but also to the right to mobility and to the legitimate right to protest.

Lawyer Laia Serra highlights the legal and ethical problems posed by the increasingly sophisticated nature of the surveillance, and asks, “*Why do local councils want cameras with such advanced recognition systems, if their only mission is, in theory, to prevent or avoid incidents?*”

In many other cases, CCTV and video sensors are deployed in neighbourhoods with a high population of migrants and racialised people, enabling the devices to contribute to racial profiling and deportation, which has been denounced by organisations such as Irídia and Novact in a recent report.³⁸ In the same vein, in Ciutat Vella, a district in Barcelona where most identity checks are carried out based on racial profiling, 13 CCTV devices were to be installed by 2020 to “guarantee security in public spaces and helping to combat terrorism”.³⁹

37 Nod050 (27 September 2009) ‘Nos espían: 48 cámaras de videovigilancia serán instaladas en el barrio de Lavapiés y Tirso de Molina.’ info.nod050.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/

The use of CCTV in public spaces may also be used to monitor the activities of political groups without a warrant, especially those surrounding political premises and squatted social centres, which are numerous in cities such as Madrid, Barcelona and Bilbao. A clear-cut case of video surveillance aimed at monitoring groups is around the emblematic squat, Kasa de la Muntanya, in Barcelona, one of the oldest in Europe. There are several CCTV cameras in the street to monitor the entrances to see who goes into the house, where political meetings are usually held with people from all over the city. In 2013, activists from the squat reported having discovered and dismantled a video camera installed in front of the house. The camera was hidden in a false ventilation pipe on a hospital roof and was able to send the recordings via a wifi connection.⁴⁰ *"The images captured by a video surveillance camera can be used in a summary if they comply with formalities of the law regulating their use, but sometimes express authorisation is not requested in order to monitor political activities, which would violate the regulation of these devices and infringe civil liberties,"* says Eva Pous, a lawyer with the Alerta Solidària organisation.

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

TREND 3:



**INTERCEPTION OF COMMUNICATIONS
AND DATA EXTRACTION
BY LAW-ENFORCEMENT AGENCIES**

Law enforcement agencies are spending a significant part of their annual budget on surveillance technology in order to track, locate, watch, and listen people in Spain, often targeting dissidents and migrants. One of the methods used to collect information is the extraction of data from personal devices, such as mobile phones, tablets and computers. Mobile Phone Extraction technologies, known also as mobile forensics, involves *“the physical connection of the mobile device that is to be analysed and a device that extracts, analyses and presents the data contained on the phone,”* according to Privacy International.⁴¹ Measures to extract and retain data from mobile phones and other devices impinge on the fundamental right to privacy. As such, they must comply with international human rights standards. However, while it is possible to detect a state and regional trend that is leading governments and service providers to accumulate an increasing

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

amount of information about citizens, controversial companies have a monopoly on these systems for data extraction, decoding and digital forensic analysis, such as the Israeli **Cellebrite**, whose Universal Forensic Extraction Device (UFED) technology is used by many European police forces, including Spain's national and regional police forces.

For now, however, the most widely used techniques are still police wires, either by hacking into mobile phone microphones or by placing physical microphones in premises. For instance, the Integrated Telecommunication Interception System (**SITEL**)⁴² is an integrated computer system for the legal interception of telecommunications at the national level and joint use by the Dirección General de Policía and the Guardia Civil, with two monitoring centres and their associated networks and remote terminals.

The Policía Nacional uses **SITEL**,⁴³ which allows thousands of calls and messages to be investigated, with judicial authorisation, in order to obtain real-time information about the interlocutors, content, messages and location. The device can record all conversations and stores them on a hard drive. Everything is encrypted, so that SITEL can only be accessed with a personal passcode.

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_tPhijiJsRpvFCwBxAkbL07/

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

COMPANIES INVOLVED

Insikt Intelligence is a technology company based in Barcelona. It creates easy-to-use tools in order to help LEAs gain vital intelligence on cybercrime. They are experts in mining social media and advanced text analytics on all digital sources, with over a decade of experience in research and development.

Insikt has developed an intelligence platform called **INVISO**, for the real-time detection of Jihadists on social media platforms.

The Catalan company has been funded by the Horizon 2020 Programme with a project called 'Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization'.⁴⁴ The project aims to pre-empt terrorist acts and fight radicalisation, making it crucial to detect cyber-propaganda early. The project ran from October 2017 to March 2020.

Insikt also participated in another European-funded project called 'RED-Alert',⁴⁵ where it combines artificial intelligence (AI) technology to collect, process, visualise and store online data related to suspected terrorists. In this project, the Spanish Interior Department participated via the Guardia Civil.

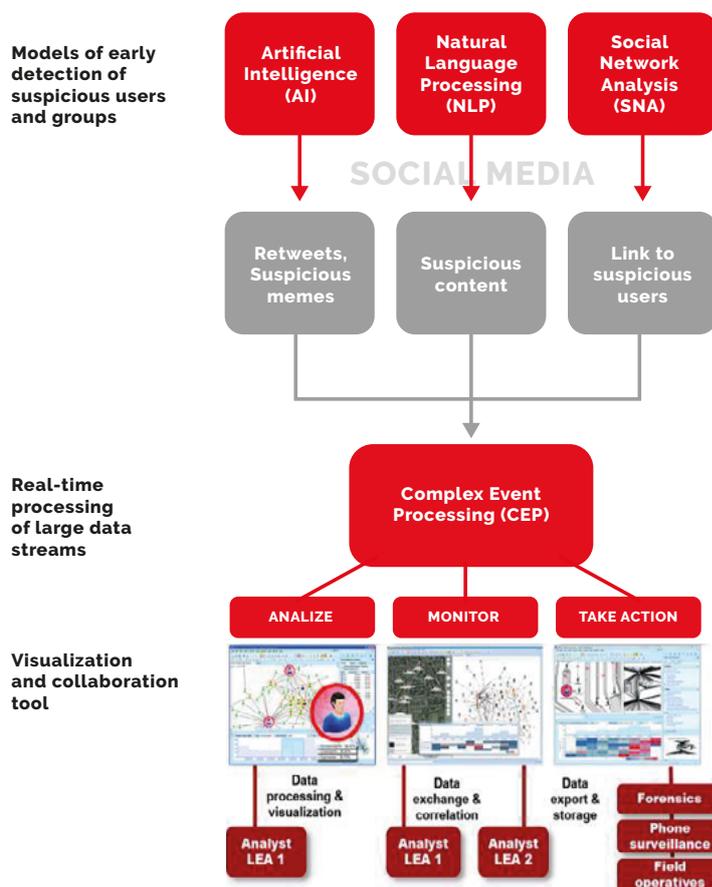
The project's advisory board⁴⁶ includes a number of experts, among whom are the former heads of European intelligence and the former director of the Security Department, who later became the Director of INTERPOL & International Operations of the Israel National Police (INP).

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/

Diagram showing the working process of RED-Alert Project. Source: RED-Alert Project.



Another ongoing project funded by the Horizon 2020 Programme is the Prediction and Visual Intelligence for Security Information-PREVISION,⁴⁷ in which several public bodies and private Spanish actors participate. The project started in September 2019 and will run until August 2021, with EU funding of €8 million.

PREVISION will provide advanced, almost real-time analytical support for multiple big data streams (from online social networks, the internet, the Dark Web, CCTV and video surveillance systems, traffic and financial data sources). There is also Spanish participation in the project, such as the Universitat Politècnica de València, the Basque Security Department and the private company **ETRA**.

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

Fortier Europe is a distributor in Spain and Switzerland for high-end professional equipment in audio, video and telecommunications. Their clientele in Spain is mainly LEAs. Some of the products that the company sells in Spain are labelled as 'terrorism proven'. The company has obtained many public contracts⁴⁸ in the last decade for the supply of four items of micro-IP undercover audio equipment with IP communication,⁴⁹ and GPS tracking equipment and one item of undercover audio recording equipment respectively.⁵⁰ Fortier Europe has a partnership with Cedar Surveillance to sell its products to LEAs in Spain. Cedar Audio is a British company specialised in audio products but also produces audio surveillance systems, such as the Trinity System.⁵¹

The Central Operational Unit of Guardia Civil⁵² has a system called **Egobox** made by Fortier Europe S.L. This system allows for discreet audio recording, including conversations over long distances. Egobox works in parallel with SITEL, which is also used by the Guardia Civil.

Grupo Excem is a multinational company, whose parent company (based in Spain) was originally dedicated to supplying cement for construction, is now a business conglomerate with a presence in Spain, China, France, Israel and the USA, under the name of Excem Grupo 1971, S.A.

Excem also collaborates with the Spanish armed forces, especially in the maintenance of mobile phone interception equipment. The contract is worth €347,645 and negotiated in secret, as reported by *El Confidencial Digital*.⁵³

According to sources consulted by *El Confidencial Digital*, the system to be maintained is the **Verint System**, developed by the Israeli-US company **Verint**. This system allows any LEA to use portable tools to 'interrogate' mobile phone lines and determine, among other things, who owns a particular phone, where it is located or to extract data from a device.

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-telefonico-as/20170116184112084093.html

Verint became infamous in Spain in 2012, when its products were used by the company Interligare to allegedly spy on leaders of the Spanish right-wing political party, Partido Popular.⁵⁴ According to a Privacy International report, in 2014 Verint sold highly developed surveillance technologies to Kazakhstan and Uzbekistan together with another Israeli company, NICE Systems.⁵⁵

At a regional level, and given public security role of the Mossos d'Esquadra, the Catalan Police acquired a system made by Excem⁵⁶ that allows them to intercept and monitor communications.⁵⁷ This is one of the Catalan Interior Department's largest contracts, worth several million euros. The Interior Department has called this system, *Sistema d'intercepció legal de les comunicacions (SILTEC)*.

The communications intercepted by the Catalan Interior Department have used technology supplied by Excem, which also supplies SILTEC and has been responsible for its maintenance since 2010. Excem also supplied the two items of portable mobile interception Verint equipment, which was allegedly acquired by the Mossos a few years ago.

S21Sec is one of the first cybersecurity companies with operations and offices in Portugal and Spain. On its LinkedIn site, it defines its business as the largest Iberian cybersecurity company.⁵⁸ The firm participated alongside the Catalan Police in the European CAPER PROJECT,⁵⁹ whose goal was to create a common platform for the prevention of organised crime through sharing, exploitation and analysis of open and private information sources.

The CAPER project was supported by the European Commission through the Seventh Framework Programme for Research and Technological Development with up to €5.6 million of a total budget of €7.1 million. The three-year project ended in 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/2012080901000066200.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/

Through the Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) of the Generalitat de Catalunya, Mossos d'Esquadra acquired a system made by the Israeli company **Voyager Labs**⁶⁰ and distributed in Spain by S21Sec, which is based on AI and used to carry out internet threat research strategies focused on combating Jihadist terrorism.⁶¹ The contract started in July 2020, so the consequences will be seen in the near future. The contract was made under an 'emergency' procedure – without putting it out to tender or allowing another company to apply – claiming 'national security reasons', as stated in the file.⁶²

According to its website, one of its key products is **Voyager Analytics**,⁶³ a system that can analyse "immense amounts of data" to determine the relationship networks, behaviour and preferences of a particular individual, the interests of a group, its links and members, the role each plays, and key event figures and the extent to which they may be a threat.

The other technology developed by the company is called **Voyager Check**,⁶⁴ which uses machine learning and natural language algorithms to generate alerts or answer specific questions. The company says it allows for an "almost real-time" response, even if it deals with information from millions of people.

The company is expanding, and in May 2019 it inaugurated its new security operations centre in Madrid where all the activity and cybersecurity incidents that occur inside Spain and beyond will be monitored in real time.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. contractaciopublica.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 is a leading digital forensics company founded in 1999 in Petah Tikva in Israel,⁶⁶ hugely popular among government agencies and states. The company is currently a subsidiary of Japan's **Sun Corporation**, although its headquarters and executive team remain based in Israel. The company's most widespread and famous device, UFED, is capable of accessing and extracting data exploiting vulnerabilities from a wide range of digital devices to collect information such as wifi networks, location and cloud data from mobiles and GPS devices. Cellebrite UFED logical extraction can also recover deleted data, according to its website. The Israeli company supports national and transnational police forces – such as the FBI,⁶⁷ Interpol⁶⁸ or Europol, intelligence services, border patrols, special and military forces and financial organisations in more than 100 countries.

In other European countries that are increasingly using smartphone surveillance to control the movements of asylum seekers, Cellebrite offers its technology to audit a person's journey to identify suspicious activity prior to arrival, track their route, run a keyword and image search through its device to identify traces of illicit activity.⁶⁹

In the case of Spain, Cellebrite has been used by the Guardia Civil to hack the phone of Josep Maria Jové, a Catalan politician arrested for allegedly organising the 1st October referendum and who refused to give his password to the officers.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

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

Intrusive police interception and GPS location

The surveillance of activists by Spain's police forces is by no means just an anecdote. However, some cases deserve special mention because of their seriousness and their enormously damaging consequences for the right to privacy and the secrecy of communications.

Between 2013 and 2015, the Guardia Civil, the National Police and the Catalan regional police opened a series of macro-operations against anarchist groups, in which 68 people were arrested. In December 2014, the first operation, code-named 'Pandora', resulted in 11 arrests in Catalonia and Madrid, as well as searches of homes and political premises, and the seizure of books, documents, computers and telephones.⁷¹ Seven of the activists were remanded in custody in Madrid for six weeks, accused of belonging to a terrorist group with anarchist ideology, until the summary proceedings were lifted. The evidence was based on two facts: possession of a booklet entitled *Against Democracy* and "using extreme security measures, such as Riseup's server," in the words of the judge of the Audiencia Nacional that authorised the warrant.⁷² Even though this use was completely legal, the police action stigmatised the use of encrypted communications as means of protection against state surveillance, making it appear as doing so was a criminal activity.

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/>

In the case of Operation Pandora I and II, which were the result of an investigation by the Mossos d'Esquadra, and authorised by the Audiencia Nacional, the people arrested had been long subjected, some of them for years, to particularly invasive and damaging police tapping, violating their right to privacy. Following the acquittal of the detainees in both raids, the judge claimed that *"the generic statements made lack a solid objective basis in the content of the conversations that have been facilitated."*⁷³ She added: *"Throughout the investigation, no indication has been given as to which specific phrases or conversations could be referring to a specific act of terrorism."* One of the anarchists arrested in the first Operation Pandora, who was also held in custody for nearly two months, explained to our researchers that – in her case – 400 messages and 261 telephone conversations were intercepted. Most of the conversations were of an intimate nature or related to her affective friendship networks.

Another of the most recent cases of police wiretapping of political dissidents was the investigation of the so-called Committees in Defence of the Republic (CDR), Catalan pro-independence grassroots groups. On 23 September 2019, the Guardia Civil arrested nine people – some of them environmental or neighbourhood association activists – in several Catalan towns, with a huge deployment of anti-terrorist police.⁷⁴ They were accused of preparing violent actions against the imprisonment of pro-independence politicians and leaders. According to one of the activists, in some cases the police officers in charge of investigating them had copies of their car keys and several of them also discovered that GPS devices had been placed on the vehicles to track their movements.⁷⁵ Her lawyer warns, *"The fact that the case file is secret prevents us from assessing whether this level of monitoring with wiretaps, microphones, GPS location, etc. was justified, since it is not known how these measures are agreed upon or the reasons for them. It is an anomaly and a danger to rights and freedoms."*

In 2015, a digital rights activist reported having found a GPS device stuck under her car, after being stopped at a police checkpoint,⁷⁶ on her way to the Circumvention Tech Festival – ironically, a conference on surveillance and privacy in Valencia.

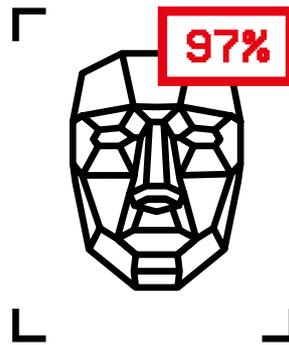
73 *Diari Ara* (15 June 2016) 'L'Audiència Nacional arxiva el cas dels activistes detinguts en l'operació Pandora II'. https://www.ara.cat/societat/Audiencia-Nacional-arxiva-investigacio-Pandora_o_1595840637.html

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 nou*, 28 August. <https://elnou.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

TREND 4:



FACIAL RECOGNITION
AND BIOMETRIC TECHNOLOGY

Facial recognition algorithms have different rates of accuracy depending on the demographic groups, according to a study published by the National Institute of Standards and Technology (NIST) in 2019.⁷⁷ NIST confirmed that a majority of algorithms exhibit demographic differences in both false negative rates (rejecting a correct match) and false positive rates (matching to the wrong person). Companies like Amazon and IBM are pausing and abandoning their facial recognition technology after years of pressure from civil rights advocates.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/

Facial recognition technology has been applied in Spain in various settings, such as bus terminals, since 2016,⁷⁹ but it has been deployed on a far larger scale during the COVID-19 pandemic.

In 2020, the Spanish Sub-secretary Department approved a Resolution, in agreement with the Centre for Technological and Industrial Development (CDTI), to install facial recognition cameras at the entrance of stadiums, concert halls and other large venues across Spain.⁸⁰

Facial recognition technology has been used in different contexts in Spain, including commercial establishments where you are able to 'pay with your face'. This system allows you to be identified by facial recognition through biometric technology and you can automatically make a payment that will be charged to the credit card with which you registered.

Facial recognition technology has also reached the world of cars. The Spanish **Antolín Group** and Israeli **Eyesight** have joined forces to launch this system in future vehicles. In this alliance, the Spanish company integrates monitoring sensors and cameras, so that this technology is not invasive. Eyesight develops all the software that allows facial recognition. Under the name **Driver Sense**, this driver monitoring system analyses the eyes, eyelids, pupils, head position and look of the driver to determine their attentiveness and alerts them to distractions and drowsiness.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://www.google.com

COMPANIES INVOLVED

Herta Security (Grupo Everis) is a world leader in face recognition and crowd identification technology. Based in Barcelona and with offices in Los Angeles, Mexico City and Montevideo, Herta has partners in 50 countries and more than 250 certified integrators worldwide. Herta Security was a spin-off from the Universitat Politècnica de Catalunya. Some of its projects include safe cities, airports, train and metro stations, prisons, banks, casinos, sports stadiums, shopping malls, military, police and forensic applications. The company belongs to the Everis Aerospace, Defense and Security group.⁸²

Herta is specialised in the analysis of crowded environments, making it possible to detect and identify multiple subjects at the same time through IP cameras.

The company is quite new, starting its activities in 2009, so its international reach is astonishing. Herta Security has won public contracts in Spain and elsewhere. Border controls have also become part of Herta's business. Herta has developed a project in Phuket (Thailand) that was intended to identify people going to the country or city by motor vehicle in order to reduce crime rates.⁸³ At the security checkpoint, the police use their mobile phones to take a picture of all of the passengers on the vehicles coming into the city. Then, the picture/video streaming is transferred via wireless Access Point (AP) to the network of Herta's **BioSurveillance NEXT system**.⁸⁴ Every time a blacklisted subject is detected, the system sends an alarm to the security guards' mobile phones.

In Spain, Herta Security products have been used at the largest bus terminal since 2016⁸⁵. According to the company, the system has been a success ever since its implementation, given the 75% reduction in incidents.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/

The facial recognition products are also being used in Casino Gran Madrid.⁸⁷ The system comprises three **Axis** cameras with capabilities specially designed for facial recognition, using wide dynamic range (WDR) technology that enables identification even under backlighting conditions or when bright light sources are in view. This server-based facial recognition system is fully integrated with the casino's video surveillance. From the control centre it provides direct facial view of the last individuals to have entered the establishment, the ability to perform quick searches, etc.

Herta Security has contacts with international institutions in Europe and has been coordinating an EU-funded project called AWARE, which analyses crowd behaviours,⁸⁸ and can be integrated into any type of camera.

Thanks to this project, In May 2020, Herta was awarded the **COVID-19 Seal of Excellence** certificate by the European Commission.⁸⁹

Thales SA is a France-based technology company, offering services in three areas: Aerospace, Transport and Defence and Security. **FRP**⁹⁰ is Thales' state-of-the-art biometric face recognition system. It is an algorithm based on deep neural networks for face detection, tracking, and recognition. Thales is supplying this technology to Madrid's airport in partnership with **IECISA** and **Gunnebo**⁹¹. The facial recognition system has been installed at the airport's J40 and J58 boarding gates at terminal 4.

In September 2019, Thales in partnership with **Gunnebo**, a Swedish company specialised in technological security, has been selected to run a project from Spain's territories in North Africa Ceuta and Melilla, where there will be an entry-control system using facial recognition technology, in which a total of 35 cameras have been installed between the entry and exit points of each of the borders, and the Thales LFIS (**Live Face Identification System**) software platform for the control of the CCTV system.

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 This company is based in Vilassar de Dalt, near Barcelona. It specialises in controlling access and checking physical presence of people using new technologies.

Since 2012, the public High School Enric Borrás, located in Badalona (Barcelona), has been using "a system of facial recognition and the sending of SMS to families to control the attendance of students", according to the Badalona Educational Information Guide for the 2019–2020 academic year.⁹²

Veridas The company based in Navarra was founded in 2017 as a joint venture between BBVA bank and **das-Nano** (tech supplier of the High Security Printing Industry). They are experts in Digital Verification of Identity and have developed technology for Face Biometrics, Voice Biometrics and Identity Document Verification. As well, for the Spanish bank BBVA, it has developed a facial recognition technology that allows its customers to pay after biometric recognition. The bank has launched a pilot project in Madrid that uses facial recognition based on biometrics to allow employees to make payments without having to use either a credit card or smartphone. Customers have to stand in front of a booth with a camera that recognises their face – previously registered in the application – and the payment is made automatically.⁹³

Bee the data is a start-up that began trading in 2015 and is based in Barcelona.⁹⁴ It has been developing software through AI cameras and algorithms that capture, analyse and understand human behaviour in physical areas. The project's website says that LEAs awarded the company a mention of honour.⁹⁵ It sells two products:

Behavior, which employs state-of-the-art deep learning algorithms to capture, analyse and understand human behaviour at physical points from camera feeds, and is used for business purposes.

Beeye, a mass facial recognition technology, able to detect people's unique physical characteristics, and is used for security purposes.

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 biometrics.

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 is a technology company based in Alicante.⁹⁶ In April 2016, FacePhi presented the FACCESS project through the Horizon 2020 programme, the largest European Programme for the Financing of Research and Innovation Projects.

The FACCESS project involves the expansion of FacePhi's activity in the EU by implementing facial recognition pilots in the most prestigious financial institutions across Europe.⁹⁷

The European Commission signed the contract for the development and implementation of the FACCESS project, thus approving the lost-fund subsidy that awards the company €1.69 million to be disbursed over the two years of the project. The project was also awarded the European Community's seal of Excellence, with a score of 14.48/15.

In early 2019, the company signed one of its largest contracts with the Catalan CaixaBank in order to supply its facial recognition software '**SelPhi**'.⁹⁸

Anyvision⁹⁹ is an Israeli company founded in 2015 by academic staff and cybersecurity experts and specialised in facial recognition technology. Its systems **Better Tomorrow**, **SesaMe**, and **Insight** particularly stand out. These systems are used for domestic security such as border controls, airports and by several LEAs.

Mercadona, one of Spain's largest supermarket chains, has announced the installation of what is supposedly an Anyvision facial recognition system, created to detect people with a conviction or a precautionary measure with a restraining order issued by a court to forbid them to enter the establishment.¹⁰⁰ Mercadona has installed this system in approximately 40 supermarkets in Mallorca, Zaragoza and 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/

Eyesight Technologies This Israeli company is a leading provider of AI vision systems installed inside vehicles and, together with **Antolin Group**, one of the world's largest vehicle interior manufacturers, has reached a collaboration agreement to deliver driver and passenger monitoring systems to car manufacturers.¹⁰² Eyesight Technologies have developed the **Cabin Sense** system, that monitors the interior of the car and passengers allowing customisation and adaptive safety functions. Eyesight Technologies technology also makes it possible to identify the driver and detect actions such as smoking, wearing the seat belt or using the mobile phone.

Grupo Sabico This company is headquartered in San Sebastián and has been active in the security sector since 1989. At the International Security Exhibition 2018 held in London, the company presented its facial recognition system, which recognised many of the faces of the people attending, including the Interior Minister, based on images of his public profile on social media.

According to its website and a video, the cameras used for the facial recognition software are from **Avigilon**, a subsidiary of **Motorola Corporation**.¹⁰³ Sabico also uses Avigilon cameras on the Motorbike Aragon Grand Prix.¹⁰⁴

Since 2018, through a project¹⁰⁵ funded by the Centre for the Development of Industrial Technology and the European Regional Development Fund, Spain participates with six companies in the field of technology and security, including the Catalan Herta Security, in implementing a surveillance and control system based on 5G technology and AI, and facial recognition technology to the point of developing algorithms to identify abnormal behaviours. The outcomes will be available to law-enforcement and private security officers. Indeed, the Guardia Civil collaborated with the project, with a budget of €5 million until 2022.¹⁰⁶

¹⁰² Eyesight. '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

The AI MARS project facilitates the adoption of technological solutions to provide immediate information to public and private security forces and bodies as well as managers of large public spaces (commercial centres, sports arenas, etc.) to prevent attacks, crowding, riots and other incidents in large concentrations of people and other situations with high security requirements. This technology, as explained by one of the project's participants on the company's website, is also applicable to border control and the protection of critical infrastructure.¹⁰⁷

Another way to get into the European market are the tech clusters and Joint Ventures. As described earlier, the 'Payment Innovation Hub' in Barcelona is a joint venture by CaixaBank, Global Payments, Visa, Samsung and Arval to develop R&D projects, and have established a system to pay 'with the face' and to withdraw money from ATMs after a biometric check.¹⁰⁸ Lanzadera is an initiative of Juan Roig, the owner of Mercadona, located in the Valencia Marina, with the aim of training, advising and financing entrepreneurs. Among the start-ups funded by Lanzadera, several are working with AI to develop facial recognition technology.

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

¹⁰⁸ R. Sampedro (2020) 'CaixaBank multiplica los cajeros que reconocen caras'. *Expansion*, 6 June. www.expansion.com/empresas/banca/2020/06/06/5ed19581e5fdea6b3b8b45bd.html

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

Facial recognition against activists

The impact of facial recognition technology and other biometric systems on political rights has yet to be fully determined, as their widespread use in public security is relatively recent. So far, it is known that – in the hands of state security forces – they have been used to collect images at political protests to identify demonstrators and to check activists' faces against databases of criminals and terrorists or to provide images as evidence in trials.

Although the justification for collecting images of demonstrators in political protests is the commission of criminal acts, in Catalonia, the Basque country¹⁰⁹ and other parts of Spain,¹¹⁰ activists are recorded before the rallies take place or even during peaceful demonstrations. Alerta Solidària, linked to the Catalan pro-independence left and other anti-repressive organisations, has reported that the autonomous police of Catalonia carried out “illegal preventive identifications” of those who try to attend protests, such as the celebration of the National Day of Catalonia, by requesting their identity cards and police officers recording faces and clothing with handheld cameras.¹¹¹

The startup Bee the Data S.L. has an application which allows the user to compare and search for matches between the images taken and the databases of repeat offender or wanted terrorists at international level.¹¹² According to the media, the Catalan police decided to take over the facial recognition application of Bee the Data S.L., but did not acquire it directly or through public tender, but in a framework contract with T-Systems, and purchased for €500,000.

Despite the lack of neutrality and overall credibility of this source, the Lanzadera start-up support platform also acknowledged on its website that state police forces acquired the Bee the Data facial recognition software in 2017 and that, in 2018, the security forces awarded it an honorary mention.¹¹³

In several cases, these images have later been used in political trials, where features such as the shape of the ears or the contour of the eyes were used as evidence to indict activists. As argued by Laia Serra, a lawyer specialising in human and fundamental rights, the use of these cameras is never two-way, since

¹⁰⁹ Asociación anadaluz 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 il·legals' 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/

“the images provided as conclusive proof of an activist's presence in a protest do not weigh the same in order to identify an agent who commits an abuse of power or aggression” in a territory where the use of rubber bullets has resulted in the loss of an eye on more than 15 occasions. In the vast majority of cases where images taken by the police or by photojournalists have been provided to identify the officer guilty of this serious violation, they have been rejected as definitive evidence. “There is a total lack of control by citizens and rights defenders over what use is made of the images that are massively collected in political protests, in many cases with state-of-the-art technologies. There is also a lack of control over how this information is stored, shared or destroyed or what kind of databases are being fed,” confirmed the lawyer to the authors of this report.

This type of collection of activists' images is not only taking place in violent protests, but is spreading to all kinds of political events. *“I have witnessed people being filmed attending evictions without any infraction, so they are being recorded for exercising their political rights. No one ever explains what the use and destination of these images is”*, claims Serra. *“The use of facial recognition software is not specified in the court files, but we suspect they are used because when dozens of activists are arrested after a protest and shown a huge number of photographs, it is impossible for the police to have processed these images manually,”* says Eduardo Cáliz, a lawyer for the social movements.

DNA illegal gathering

Several lawyers and activists recall that, at the height of recent political protests in Catalonia, the regional police admitted in some trials that they had stolen personal objects – such as toothbrushes – from people being evicted, in order to obtain their DNA. This practice was diluted, at least in cases of protests and political crimes, with the adoption of the General Data Protection Regulation (GDPR) in 2016 and the domestic legislation that followed. However, it was precisely in 2016 when one of the clearest cases of dubious procedure in collecting DNA from activists took place.

In April 2016, the Catalan police broke into a well-known squat on the instructions of the Spanish National Court.¹¹⁴ An international rogatory commission had been processed, conducted under the secret summary proceedings at the request of the public prosecutor's office of the German city of Aachen, and it ended with the arrest of a woman, Lisa. She was an anarchist activist who had a European arrest and surrender warrant for the criminal police of the German state of North Rhine-Westphalia, accused of robbing a bank.

Laboratory analysis of genetic samples obtained from traces found in a wig and other pieces of clothing, abandoned in the vicinity of the Aachen bank after the robbery, provided DNA profiles to the police. These traces were sent to other European states to look for possible matches in their genetic databases. Months after the event, the Catalan police warned that they had detected a hypothetical match between one of the genetic profiles found on the wig and an – albeit anonymous – entry in their register. At the time, the use of this methodology by the police in Catalonia to increase control over social movements was uncertain, but was somewhat corroborated by the event in Aachen and the relationship established between these events and direct political action in Barcelona in June 2009. Police officers at the political demonstration collected evidence at the scene and found a glove, from which they obtained a genetic trace. The sample remained in storage, without being identified for years, until the alarm was sounded when the trace was crossed with the profiles obtained by the German police at the bank in Aachen.¹¹⁵

¹¹⁴ ElDiario.es (13 April 2016). 'Los Mossos detienen a una persona en una operación contra un Centro Social de Barcelona'. https://www.eldiario.es/catalunya/persona-detenido-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/

As they needed to confirm the triangulation to incriminate Lisa, a group of plain-clothes police officers followed the activist on a summer night in the streets of Barcelona, secretly picking up an empty beer can that she had left on the street. According to Lisa's defence lawyers, the genetic profiles had been obtained potentially illegally and without the authorisation of a judge,¹¹⁶ as they argued at her trial in Germany.

But the emblematic laboratory for collecting DNA for political reasons has historically been the Basque country. Since 2000 in particular, with the emerging phenomenon of street violence or *kale borroka*,¹¹⁷ the Basque police began to use genetic testing to indict dozens of young people in court proceedings, which resulted in some of them still serving exceptionally long prison sentences.¹¹⁸

This fact led to the discovery that the regional police had been building up a database since the 1990s with hundreds of fingerprints and DNA traces collected at the site of attacks, to be compared with others that were often obtained without a warrant.

¹¹⁶ Ibid.

¹¹⁷ A strategy based on generating low-intensity violent street confrontation.

¹¹⁸ Oscar B. de Otilaor (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

TREND 5:

**AUTOMATIC NUMBER PLATE
RECOGNITION (ANPR)**

46

Whether you are driving, taking public transport, or just walking along the street, one thing is certain – you will be filmed. In this context, ANPR¹¹⁹ cameras appear with the technology to identify vehicles. These cameras do not simply photograph the number plate but the entire vehicle. It is just a question of time in Spain that each occupant of the vehicle can be identified with an additional facial recognition module.

ANPR cameras are able to read number plates and to record perfectly visible snapshots of running vehicles (even those driving at high speeds) because of their remarkable shutter speed, commonly 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-matriculadas-anpr

The system consists of two license-plate readers installed on the roof of the police patrol car, near the blue lights. The cameras record all the license plates they see around them. From each license plate, the system extracts numbers and letters and feeds them into the computer equipment in the patrol car in order to check personal data.¹²¹



Pictogram showing the functioning of the ATHENA system.

COMPANIES INVOLVED

Federal Signal is a company specialised mainly in signage, but also has an important portfolio of products for police forces. In Spain it distributes a system called **ATENEA**¹²² for the total control of signalling systems, surveillance, etc. This system facilitates control all the luminous and acoustic devices, communications, data management and analysis, makes audio and video recordings, etc. in the most adverse environmental and visibility conditions. The ATENEA system consists of various applications that assist the emergency professional, including **FEDRECOGNITION**, the automatic recognition system of ANPR number plates.

In 2019, the company provided the Guàrdia Urbana of Barcelona with 15 pairs of automatic ANPR cameras.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 Seguridad¹²⁴ is a security company specialised in conducting AI photographs of vehicles that may have committed a traffic offence. These images are shared with the Law Enforcement Agencies. It also distributes license ANPR systems. One of its most important clients is Guardia Civil.¹²⁵

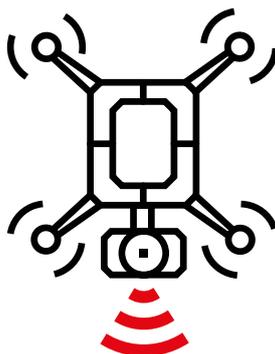
IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

Just as it is a matter of time that each occupant of a vehicle will also be identified with facial recognition technologies, it can be assumed that the possibility of obtaining more information about the passengers will be used for law-enforcement purposes, not only against criminal networks but also against political dissidents. At present, however, there are no documented cases.

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

TREND 6:



DRONES SURVEILLANCE¹²⁶

In December 2017, the Congress of Deputies approved the Royal Decree 1036/2017, the new law on drone regulation, issued by AESA (State Aviation Safety Agency), which expands and specifies the legal framework in the face of the great growth of a sector that has over 3,000 professional licenses across Spain. Bodies such as the Dirección General de Tráfico (DGT), the National Intelligence Centre (CNI), Customs and State Security Forces are exempt, although they do have to respect minimum standards.

In a press release issued in 2018, the DGT made clear its willingness to acquire drones for traffic control. This sphere has become one of the biggest markets for drones in coming years.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

Drones are also used to control the population in Spain. Many local police forces in Spain have, during the lockdown due to COVID-19, used drones as a new means of control and vigilance. Drones have been used to give recommendations to citizens as well as to monitor evictions and access to mass events. The Spanish police was among the first LEAs in the world to use remote-controlled drones for surveillance of the population.

Drones were first used officially by law-enforcement agencies at the 2018 Mobile World Congress (MWC) by Mossos d'Esquadra, which established the first operational surveillance drone to ensure public safety.¹²⁸

The Guardia Civil was one of the LEAs which used drones during lockdown to control people's movement following the State of Emergency measures. In the Canary Islands, Air Service helicopters and drones monitor each stretch of coastline to avoid people potentially going to their second home, excursions to the beach and other prohibited activities such as fishing or camping.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

COMPANIES INVOLVED

DJI¹³⁰ DJI is a private Chinese company and the world's top vendor of Unmanned Aerial Vehicles (UAV), controlling two thirds of the global market. The company specialises in civilian UAVs and aerial imaging technology.

DJI's official distributor in Spain, DJI Ars Madrid, supplied the Military Emergency Unit (UME) with two units of its Agras drone for fumigation in the fight against COVID-19.¹³¹

In January 2020, the Ministry of Defence confirmed that Spain is not operating any DJI drones after being questioned by *El País*.¹³²

Paukner Group For 40 years, A. Paukner S.A. has provided drone equipment and services to the Security and Defence sectors in Spain.

Before the State of Emergency, in April 2017, the Guardia Civil awarded Paukner Group a contract to acquire a tactical drone. This small unpiloted aircraft, according to specialists, is capable of making "very high quality" recordings at a great distance.¹³³

GDU Technology, The Chinese company GDU-tech, through its marketer in Spain, Droneless, has been helping LEAs in Barcelona, Madrid, Matadepera, Parets del Valles and Sabadell.¹³⁴

In addition to the vision cameras that are usually carried by drones and allow aerial surveillance, the GDU SAGA drone can carry a 120-decibel speaker, making it possible to alert and send live messages over long distances. It also has a Thermal Imaging Camera (IR) that makes it possible to take body temperature remotely.

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. 'Policia contra COVID-19'. www.droneless.net/policia-contra-covid-19/

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

Use of drones to monitor political demonstrations in Catalonia

As with facial recognition, the major threat posed by drones stems from their intrusive and invasive nature if they are used to obtain massive information or images in an illegal or non-consensual manner. Again, this concerns the right to privacy and, with the increase in social control and the traceability and monitoring of citizens,¹³⁵ has been reinforced in the context of the pandemic.

The pandemic has clearly accelerated the use of drones with features applied to restrictive measures, such as maintaining so-called social distancing. Practically all the police forces in Spain, including some local police, have flown these devices to control possible infringements and fine those who commit them, without considering the situation and its context. Some of the drones that have been set in motion, such as those of the Municipal Police in Madrid, even had thermographic cameras,¹³⁶ capable of measuring body temperature to detect people with fever, regardless of whether this was the result of COVID-19 or other more frequent infections.

In the use of drones as a control mechanism, however, the pandemic has only exacerbated a growing trend, which began in 2018 when the Catalan police flew drones to control airspace during the Mobile World Congress in Barcelona.¹³⁷ In October 2019, the regional police used their six DJI drones to control large demonstrations against the prison sentence served on Catalan politicians and sovereigntist leaders. These aircraft provide complementary images to those taken by the police helicopters, which are also equipped with high-resolution cameras. Images are sent to the command centre that makes the decisions.

One case in which this technology was most clearly used with application to public security and the control of political dissent was the Barça–Madrid match in October 2019 at Camp Nou, where a drone was capturing images of the protest organised by a peaceful resistance movement called Tsunami Democràtic.¹³⁸

¹³⁵ Revista Ideas, May 2020. 'Inteligència artificial en temps de pandèmia. Punts dèbils i oportunitats de la COVID-19'. revistaidees.cat/inteligencia-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

TREND 7:



**CRIME PREDICTIONS
SOFTWARE**

One of the priorities of law enforcement is to anticipate possible criminal acts with the aim of maintaining order at local and national levels. This task has historically lain in to analysts, however, since the late 1990s and with the development of Big Data and AI, security forces have begun to develop computer programmes and methods capable of predicting the circumstances of commissioning a particular crime.¹³⁹

The technical term is predictive policing, or predictive analysis, "the use of analysis techniques, in particular quantitative techniques, to identify potential objectives that require police intervention, as well as preventing crimes or resolving past crimes through statistical forecasts", and is based on the principle of repetition, according to the idea that criminal offenders tend to develop repetitive behaviour when their criminal method works.

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/.

COMPANIES INVOLVED

EuroCop Security Systems¹⁴⁰ is a computer system engineering, development, integration and maintenance company that provides technological support to LEAs and security-related companies.

The company has a strong relation with municipalities, gaining many contracts in recent years.¹⁴¹ One of its business lines is to supply and install video surveillance systems that can read number plates that are fully integrated with their own local police system.

EuroCop has developed a system for the prediction and prevention of crime called **EuroCop Pred-Crime**. This is an integrated system, processing massive data linked to crime and minor offences, based on a space-time model and geographic information of heat maps, and using mathematical models and algorithms and that will allow the prediction and prevention of crimes.

Bismart¹⁴² is a consultancy company on Data Management and Analytics. The company has developed a tool called **Crime Prediction**, a new solution for smart cities for drug prevention and detection. The technology makes use of predictive analytical models and sensors through an area after monitoring continuous data for a long time.¹⁴³

According to Albert Isern, CEO of Bismart, *“Advances in data analytics and machine learning now make it possible to analyse data stocks, which helps departments to identify not only where crime is likely to occur, but also when and under what circumstances.”*¹⁴⁴

As we have already seen, the Horizon 2020 Programme is funding the kind of technology represented by the Deep AR Law Enforcement Ecosystem **DARLENE**.¹⁴⁵

The EU-funded DARLENE project aims to offer European LEAs a method of proactive security that enables them to sort through massive volumes of data to predict, anticipate and prevent criminal activities. To achieve this, the project will combine augmented-reality (AR) capabilities with powerful machine-learning algorithms, sensor information-fusion techniques, 3D reconstruction, wearable technology and personalised context-aware recommendations.

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 detectar 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.

The project started in September 2020 and will continue until August 2023. There are several Spanish participants: Valencia Municipality, the Basque Government Security Department and the Centre Tecnològic de Telecomunicacions de Catalunya.

VeriPol¹⁴⁶ is software developed by Miguel Camacho, a Policía Nacional inspector. VeriPol assesses the veracity of complaints filed with the Spanish national police. It was introduced in 2018 after a member of the police force attended a PhD course on predictive policing at the University of California. The programme extracts useful characteristics from reporting narratives using natural language processing techniques. This data is processed by a mathematical model that estimates the probability of the complaint being false.

In addition, VeriPol extrapolates and identifies behaviour patterns from the data, allowing Policía Nacional officers to understand the characteristics that differentiate true and false reports. VeriPol is currently available in about 240 police stations operated by Policía Nacional.

¹⁴⁶ R. Álvarez (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

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

According to Sheila Queralt, a forensic expert specialising in police language and Director of the company SQ Forensic Language in Barcelona, the allegations scanned by VeriPol are written by agents in the police stations themselves, which means they go through an initial filter before they are processed by the computer programme. This, coupled with the way the algorithm was trained (a specialised agent defined whether or not the allegations were false), shows that “the parameters analysed are not objective”.¹⁴⁷

In Spain, these technologies are being deployed by police forces such as the Castellón Local Police, which is using a pioneering tool that makes it possible to transfer to a map the risk of the commission of a particular crime.¹⁴⁸ By basing these systems on context-free naked data, in addition to neglecting the importance of prevention, it can lead to stigmatising particular neighbourhoods and treating them as crime scenes, rather than working to prevent the structural causes that may facilitate crime. On the other hand, some of the activities carried out by dissident political groups are considered formally criminal – for example, under laws that openly limit rights and freedom, such as the 2015 Citizen Security Law – so crime-prevention technologies can clearly result in greater persecution and harassment of social movements.

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



CONCLUSIONS



It is undeniable that the power of mass surveillance and population control technologies has expanded over the past two decades under the justification primarily of the “fight against terrorism”. Supervision of communications; storage of a large amount of private citizen data; proliferation of CCTV cameras with increasingly sophisticated recognition systems; location with GPS positioning systems; implementation of technologies based on the digital footprint, facial features or reading of the iris. However, limitations on the use of these types of invasive technologies have been falling at the same rate that hindered the defence of human and fundamental rights.

The precarious balance between security and freedoms now clearly turns towards a normalisation of the invasion of all spheres of our privacy, a trend that the current health crisis has accelerated.

The concept of “Smart Cities” is another excuse to apply these types of technologies. In Spain, the government, through the initiative Red.es¹⁴⁹ and its Digital Agenda, is clearly betting on the implementation of Smart Cities, especially through the National Smart Cities Plan, with a budget of €188 million.

Even Catalonia has its own Smart City strategy, Smart Catalonia,¹⁵⁰ which is in line with the European Commission's Europe 2020 strategy.

Smart Catalonia intends to make Catalonia an international ‘Smart Country’ of reference, using digital information and technology to bring innovation to public services, drive economic growth and promote a smarter, more sustainable and more inclusive society.

Barcelona, as capital of Catalonia, has taken steps to become a ‘Smart City’ as it has signed several agreements with various technological companies such as Huawei. In 2019, Barcelona City Council and **Huawei** signed a Letter of Intention to collaborate in facilitating investment for innovative new technology projects in the city. The collaboration was signed in one of the largest ‘smart showcases’ in the world, the Smart City Expo World Congress (SCEWC) that took place in Barcelona in 2019.

¹⁴⁹ Red.es 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/

In Spain, local authorities collect huge volumes of data on citizens and visitors without their knowledge. There are numerous examples of this information being gathered without anyone realising it: smartphone data, traffic sensors, cameras, etc. These 'Smart Cities' projects are also supported by the European Commission as part of the 4ALLCITIES Project in the framework of the Horizon2020 Programme: Smart Spaces Safety and Security for All Cities¹⁵¹.

Almost all the data that is being collected and used, is taken without citizens' authorisation. It is very difficult for anyone to give permission since it is not clear exactly which data are being collected, nor the reason for doing so. The local authorities cite various objectives for their 'Smart Cities' initiatives: advertising, tourism, sustainability, mobility, urban development and safety, but the scope within which this information will ultimately be used, remains unclear.

Furthermore, all the technologies that have been described in this report have the potential to be interconnected to police command and control centres, conferring more 'power' on the LEAs and the state to control its citizens.

This report identifies a tendency to expand surveillance systems and movement control technologies, a trend that the COVID-19 pandemic is contributing to normalise and legitimise, probably permanently and without accountability, tools that allow monitoring of possible abuses of power committed by the State public security forces and companies that control and store all this data.

As some Catalan civil society organisations such as Iridia and Novact have already indicated, "the struggle for COVID-19 control is contributing to the acceleration of the development of new biometric surveillance systems in public spaces. The data collected is systematised into databases that classify people by assigning risks that individual poses to society".¹⁵² All these measures, probably necessary in the short term, call for a change of dynamics once the pandemic is under control. The long-term response to this crisis will depend on how cities react to the need to meet essential but partially conflicting needs: security and freedom, privacy and access to data. The concepts of the Smart and Safe City seem to be another excuse for the ongoing securitisation process.

The enormous health, political, social, economic and even cultural impact that COVID-19 has generated in our societies will be overcome, but the social control technologies that came with it, seem to appear to be here to stay.

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

152. Iridia 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

ENCIENDE,
TU MENTE
MUNDODESPIERTA.COM
MUNDODESPIERTA.COM

Images:

Cover page:
Fotomovimiento_Joanna Chichelnitzky,
Diada de Catalunya 2020

Inside cover:
Lucía Armiño

Page 4: Photomontage.
Original image:
Juan Lupión_Wikipedia Commons

Current page:
Barcex_Wikipedia Commons,
Demonstration 12/05/2012
Madrid



ABOUT THE ORGANIZATIONS

ENCO (European Network of Corporate Observatories) is a network of European civic and media organisations dedicated to investigating corporations and corporate power.

<https://corpwatchers.eu>

The **Multinationals Observatory**, based in Paris, is an online platform that provides resources and in-depth investigations on the social, ecological and political impact of French transnational corporations.

<https://multinationales.org>

The **Observatory of Business and Human Rights in the Mediterranean (ODHE)**, based in Barcelona, is a Suds and Novact project that aims to expose corporate-related human rights' impact and complicities in occupation and armed conflict contexts.

www.odhe.cat

Shoal is a radical, independent co-operative of writers and researchers. We produce news articles, investigations, analysis and theory-based writing as a contribution to, and a resource for, movements that are attempting to bring about social and political change.

www.shoalcollective.org

In association with:



With the support of:



**OPEN SOCIETY
FOUNDATIONS**