MASS SURVEILLANCE
AND CONTROL OF EUROPEAN DISSIDENCE

FRANCE

In France, pandemic and security discourse feed surveillance

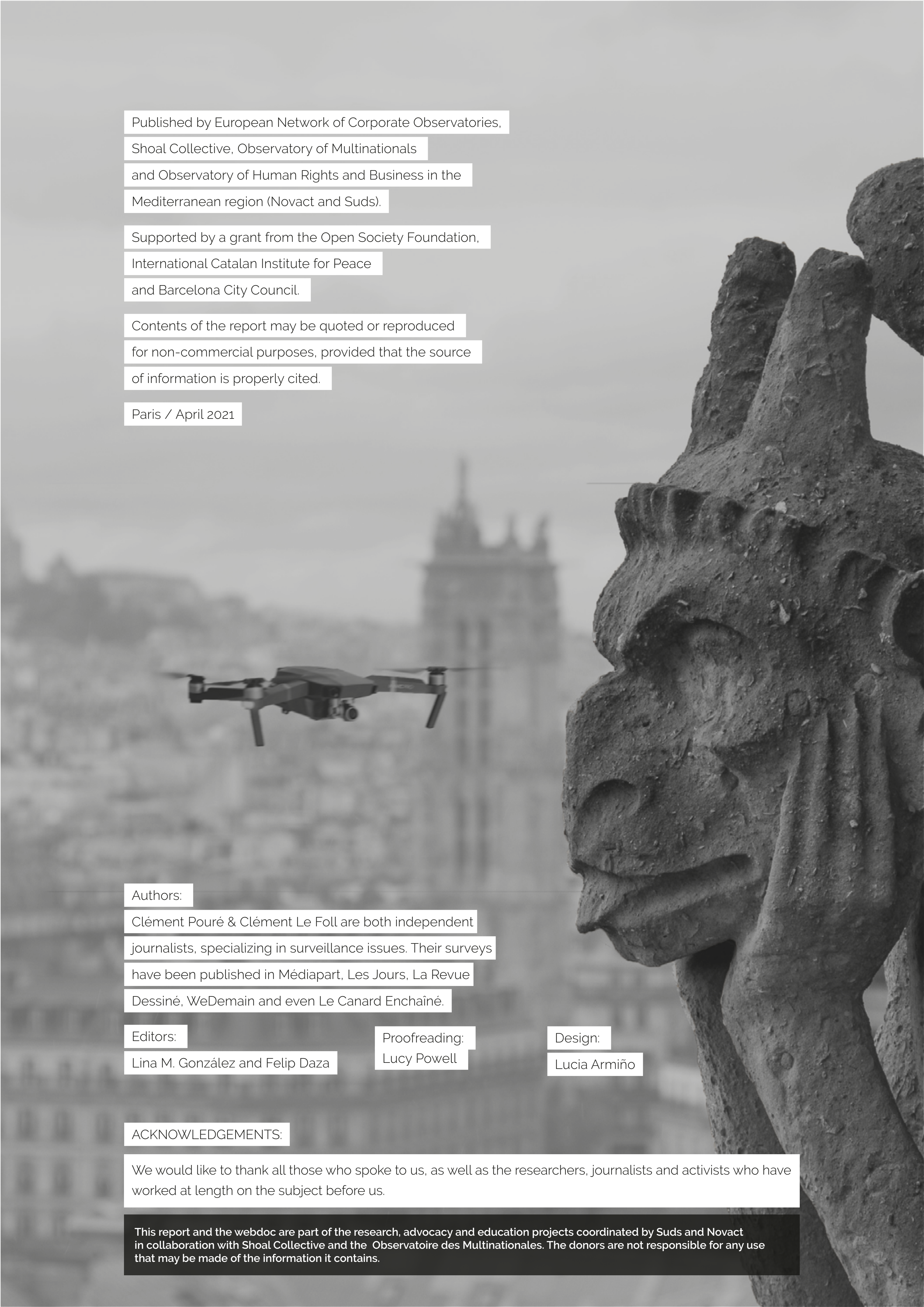
How COVID-19 accelerated the surveillance of public space and citizens

ENCO EUROPEAN NETWORK OF CORPORATE OBSERVATORIES

Observatoire des multinationales social, écologique, politique

ODHE Observatori de Drets Humans i Empreses a la Mediterrània

shoal radical writing for a world beyond capitalism



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.

Paris / April 2021

Authors:
Clément Pouré & Clément Le Foll are both independent journalists, specializing in surveillance issues. Their surveys have been published in Médiapart, Les Jours, La Revue Dessiné, WeDemain and even Le Canard Enchaîné.

Editors:
Lina M. González and Felip Daza

Proofreading:
Lucy Powell

Design:
Lucia Armiño

ACKNOWLEDGEMENTS:

We would like to thank all those who spoke to us, as well as the researchers, journalists and activists who have worked at length on the subject before us.

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.

CONTENTS

1
Methodology

2
Introduction

5
Trends

6
Safe City,
a digital city
in the service of security

11
With the pandemic,
surveillance drones
are invading public space

18
Facial recognition
and biometrics

24
CCTV & AI

29
The pandemic as a pretext
for police registration

34
Increasing centralisation
of health data

38
Conclusion

METHODOLOGY

Our objective with the research has been to provide an overview of mass surveillance in France with a focus on its concrete impact on individual freedoms.

We have used the following methods during the research process:

- Compiled information from official documents of companies and associations representing the security and surveillance sector;
- Used official documents, recovered by us during various surveys carried out throughout 2020, from administrations, communities or companies, as well as those put online by the various associations for the defence of public freedoms, in particular La Quadrature du Net and their Technopolice platform;
- Worked with press articles from the French-speaking press.
- Exchanged with industry players, researchers and activists specialising in surveillance and security issues.

INTRODUCTION

It was the middle of the first confinement. **Two-I**, a company specialising in hypervision software, announces, with great fanfare, the release of Vigilance, an image processing and data analysis software, initially designed for city management but 'rebranded' for COVID-19 crisis.

Against a background of city mapping, alerts emerge in real time. 'Car accident', 'traffic jam', as well as 'fever', 'overcrowded station', 'no mask' and 'social distancing'. By clicking on these points, the software controller accesses the live video content. Filters allow them to check the body temperature of citizens or to consult a battery of statistics.

Datakalab, which was able to experiment with mask recognition software in several French municipalities. **MyConnect**, whose thermal cameras sold like hot cakes during the first months of the pandemic. **Thales**, the French armaments giant which has signed new contracts to deploy its facial recognition solutions in airports. Since the start of the pandemic, many French companies in the surveillance sector have transformed their technologies to adapt them to the new health challenges.

Let's take a step back. While these companies have been able to take advantage of a new market, the state, as well as local authorities, have increased the number of technological gadgets to fight the pandemic. Drones used to remind passers-by of barrier gestures or to track down those who do not respect confinement, thermal cameras intended to control access to certain buildings, tracking applications to contain the pandemic... so many tools were mobilised to resolve the threatening crisis, but also to reduce individual freedoms.

From the smallest companies to large state police institutions, 2020 marks a turning point for surveillance in France. The opening of a new market for surveillance, the emergence of public safety issues linked to the health context, and a demonstrated political will to make new technologies a central tool in the fight against the pandemic have led to massive deployments of new public space control tools, while giving credibility to marginal technologies such as intelligent video surveillance. A broad trend, against the backdrop of a security shift and a social and political crisis.

It was in the early 2000s that surveillance issues began to become a long-term issue in the French political landscape. In 1993, the mayor of Levallois-Perret, Patrick Balkany, installed the first municipal video surveillance system. The model was emulated and became popular in the early 2000s. "The 2001 municipal elections played a major role," said Laurent Mucchielli, a sociologist specialising in video surveillance. "The security argument was, for the first time, a recurring theme in municipal election campaigns."

If the number of cities to be equipped increased, the boom in video surveillance was conducted by one man, Nicolas Sarkozy. A close friend of Patrick Balkany, he is equally convinced of the effectiveness of video surveillance, impressed by the system set up in the United Kingdom, which is said to have played a key role in the arrest of suspects after the attempted attacks in London in 2005.

Then Minister of the Interior in 2005, he entrusted the Inspector General of the Administration, Philippe Melchior, with the drafting of a report entitled *Video surveillance and the fight against terrorism.* A report which questions the intended goals of the device: will it fight against delinquency and banditry? Will it reassure traders and citizens? Without answering these questions, Nicolas Sarkozy passed the law of 23 January 2006 regarding the fight against terrorism, which relaxed the conditions of use of video surveillance in the public space. This tendency was accentuated when he took over as President of the Republic in 2007 and oversaw the creation of the Interministerial Crime Prevention Fund (FIPD) which, between 2007 and 2013, would dedicate 150 million euros to the financing of video surveillance by local authorities.

In 2012, as Nicolas Sarkozy's term ended, the National Commission for Computing and Liberties (CNIL) drew up an equivocal assessment.[1] 935,000 surveillance cameras was in place in France. 827,749 in places open to the public, such as shops and 70,003 in public spaces, such as roads, squares and alleyways.

While the FIPD devoted a smaller portion of its budget to video surveillance under his presidency, the election of François Hollande did not reverse the trend. Under his leadership, the state structured the security actors through the creation of The Security Actors the Council of Confidence and Security Industries (CICS), and brings together the largest actors in the sector.

"These industrial gatherings are influential because they represent thousands of jobs. They play a key role in the development of surveillance by attempting to influence legislative process," points out Martin Drago, lawyer at Quadrature du Net, the main association for the defence of public freedoms in France.

The Charlie Hebdo attacks, and the attacks of November 13, 2015, mark a new turning point in French security policy. In the aftermath of the Bataclan attack, François Hollande declared a state of emergency for ten days. This would ultimately be extended until November 1, 2017. The use of this exceptional regime, which extends police powers and reduces citizens' freedoms, is widely criticised by associations defending public freedoms. Facilitating searches and allowing house arrest – and therefore the restriction of a citizen's freedom even before a crime is committed – is used in particular to target environmental activists and

[1] CNIL press release, June 21, 2012, "Video surveillance / video protection: best practices for more privacy-friendly systems" https://www.cnil.fr/sites/default/files/typo/document/CNIL_-DP_Video.pdf

those from the alternative left within a few days of the COP-21.[2]

Several laws would then extend the power of the police. The law on "strengthening the fight against organised crime, its financing, the efficiency and guarantees of criminal proceedings," adopted on March 8, 2016, allowed the first security measures to be established. On October 30, 2017, the law on "internal security and the fight against terrorism (SILT)" was passed, This, among other things, brought house arrest into common law.

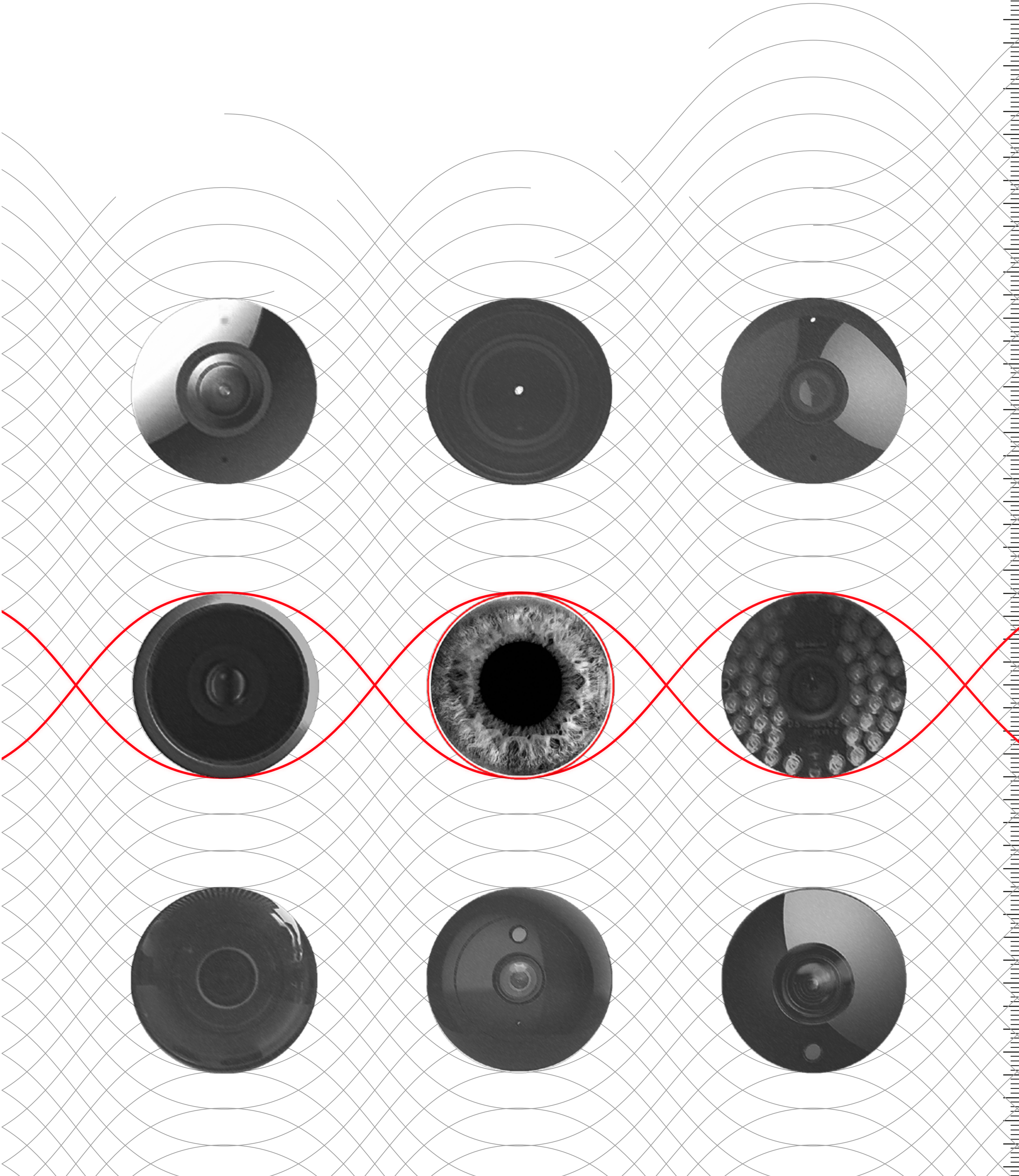
Inherited from this context of security, Emmanuel Macron's mandate was also marked by a series of security reforms. In reaction to the yellow vests movement, widely repressed and marked by significant police violence the government adopts a new law called "anti-breaker law", which, in particular, would have given police the right to ban anyone pre-emptively identified as a troublemaker from demonstrating. But France's Constitutional Council struck down this measure on April 2019.

Beyond the pandemic, the past year was also marked by major social movements against police violence, but also against the comprehensive security bill at the end of 2020. In a major reform of Emmanuel Macron's government, this bill, already adopted at its first reading by the National Assembly, is criticised from all sides for the threats it poses to public freedoms. It provides, among other things, for a ban on filming the police, the generalisation of video surveillance by drones, or even body cameras. Denounced by the defender of rights because it presents "considerable risks of infringement of several fundamental rights", the bill, which for the United Nations carries "a disproportionate infringement of fundamental freedoms," and is "likely to prejudice the 'Rule of law'", was already voted on at its first reading in the National Assembly. A security turning point that opens the door to the increased surveillance of public space.

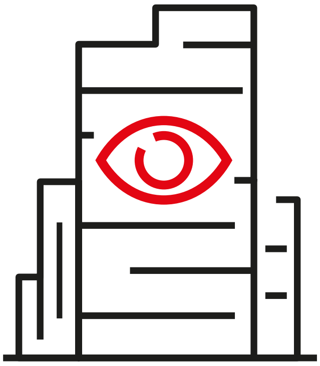
[2] Human Rights League press release, 26 November 2015, "Home Secretary loses his nerves, confuses and equates associative movement with terrorism"
https://www.ldh-france.org/ministre-linterieur-perd-ses-nerfs-confond-assimile-mouvement-associatif-au-terrorisme/

In France, pandemic and security discourse feed surveillance

TRENDS



TREND 1:



SAFE CITY, A DIGITAL CITY IN THE SERVICE OF SECURITY

At the heart of the discourse of security professionals, the ***Safe City*** is directly inspired by the Smart City, a new town model where technology is used to make public service – management of water, waste or public transport, for example – more efficient and less expensive. A way of seeing the city conceived in the early 2000s in the United States, by the companies IBM and Cisco.

The *Safe City* and Smart City are two sides of the same techno-solutionist project which claims to be able to *"govern people as one would manage a computer system,"* write Yaël Benayoun and Irénée Régnauld in their book, *Technologies everywhere, democracy anywhere*. In a *Safe City*, digital capabilities are put at the service of security. Inconvenient parking, theft, drug trafficking, crime, terrorism... no matter how serious the facts, technology is supposed to respond to this 'feeling of insecurity', an element of language abused by some politicians.

Nice is the most advanced *Safe City* in France. With 3,800 CCTV cameras, the city, led by Christian Estrosi, today possesses the most CCTV in France. Against the backdrop of a terrorist threat, the mayor is stepping up initiatives to try to strengthen the security of his city. On July 14, 2016, the National Day of France, in the early evening, a terrorist charged down the Promenade des Anglais, the city's most famous and touristic avenue, in a truck, killing 86 people. The day before, he had committed several offenses in the city, without the numerous cameras sounding the alarm.

A failure refuted by Christian Estrosi who, rather than disavowing his system, considers the mechanisms in place insufficient. The decision was made. The so-called 'martyr city' will become the first French *Safe City*, as part of a partnership with the company Thales, established in 2018.[3] For three years, the company has *carte blanche* to deploy its security technologies there. A city transformed into a testing ground, with one objective: to build a digital and monitored territory, where technology is at the service of security.

The thousands of hours of video surveillance in Nice are compiled within the Urban Supervision Center (CSU), the heart of the Nice surveillance system. Distributed over three rooms, video operators scan 90 screens in real time. The first part attempts to detect flagrant infringements. The second transcribes the images of the schools – Nice had a camera installed in front of each establishment – and those of the 900 cameras of the bus and tram network. Finally, the officers issue tickets in real time and take care of the management of road traffic. The city also has a 'security hypervisor', namely a touch screen that centralises cameras, alert buttons, traffic lights, building access controls.

As part of the *Safe City* project carried out in partnership with Thales, the city first experimented on June 27, 2019 with a flood management scenario, which mobilised connected patrol technology and focused on securing roads and schools. On December 19, 2019, visitors to the Christmas market served as guinea pigs. The next experiment, initially scheduled for November 2020, provided for an enigmatic crisis management scenario, combining predictive algorithms, a video system for analysing behaviour, a social network monitoring system and, above all, a new experiment around facial recognition.[4]

As early as 2017, another *Safe City* project was taking shape in France, in the business district of La Défense, west of Paris. Thales then planned to build a CSU, to which firefighters and police officers would be directly connected, to be able to direct their interventions. The 1,200 CCTV cameras in the business district's public spaces were reportedly linked to software which would 'detect abnormal behaviour'. Without Thales or La Défense offering any reasons, the project was ultimately aborted before even being launched.[5]

[3] Thales group website, "Nice: security at the cutting edge of technology".
https://www.thalesgroup.com/fr/monde/defence-and-security/news/nice-securite-pointe-technologie

[4] Clément Pouré et Clément le Foll (2020), Les Jours, "Nice, le « little brother » de Thales"
https://lesjours.fr/obsessions/thales-surveillance/ep1-nice-safe-city/

[5] David Livois (2017), le Parisien, "For its safety, La Défense will soon be full of sensors"
https://www.leparisien.fr/hauts-de-seine-92/pour-sa-securite-la-defense-bientot-truffee-de-capteurs-20-03-2017-6780270.php

Other communities are developing a model similar to that of Christian Estrosi's town. In December 2017, the city of Marseille thus announced the launch of its "Big Data Observatory for Public Tranquillity" intended to *"analyse what happened (in terms of crime and delinquency) to anticipate a future or likely situation"*. The project, which uses data from local authorities and law enforcement agencies, revolves around a larger system: a network of more than 2,000 smart video surveillance cameras, the use of data from public hospitals or the monitoring of social networks.

COMPANIES INVOLVED

Safe City projects are led by Thales, a company specialising in aeronautics, defence and security. Before deploying its *Safe City* project in France, Thales tested it in 2009 in Mexico City[6]. With a pharaonic budget of 460 million USD, the device has enabled the installation of 15,000 CCTV cameras, 10,000 emergency call buttons, 850 systems capable of scanning vehicle license plates and 6 supervision centres which analyse the images 24 hours a day.

In Nice, Thales is at the head of a consortium of 15 companies. The project is worth 25 million euros, including 10.9 million euros directly from the coffers of the Public Investment Bank,[7] a French organisation for financing and business development created in 2012.

Idemia is a French company born in 2017 from the merger of Morpho, the identity and security branch of the company specializing in aeronautics and space Safran, and the company Oberthur Technologies. Today, the company specialises in biometric identity. As part of the *Safe City* project in Nice, Idemia has developed two software programmes. The first is capable of automatically detecting license plates and images and identifying the colour, the make of the vehicle, as well as a sign announcing the transport of hazardous materials. The second system is responsible for detecting behaviour defined as suspicious or dangerous. *"This type of system reports accidents, vehicles in the wrong lanes and unauthorised heavy goods vehicles, and alerts an operator in a control room or performs a predefined procedure."*[8]

[6] Thales group website « Mexico : une ville plus sûre »
https://www.thalesgroup.com/fr/monde/securite/news/mexico-une-ville-plus-sure

[7] Press release from the public investment bank, "The innovative SafeCity project, to strengthen the security of smart cities in the region, obtains funding from the Future Investments Program (PIA)"
https://presse.bpifrance.fr/investissements-davenirle-projet-innovant-safecity-pour-renforcer-la-securisation-des-villes-intelligentes-sur-le-territoire-obtient-un-financement-du-programme-dinvestissements-davenir-pia/

[8] Quadrature du Net website, "Experimentation, provision and demonstration agreement: SafeCity 'experimentation project'"
https://data.technopolice.fr/api/files/1565879613407ce0u67yomk.pdf

Created in 2003, Deveryware is a French company specialising in cybersecurity. It develops real-time geolocation, anti-fraud or crisis management platforms and emergency communications. Today, the company has 140 employees and a turnover of 37 million euros. Among its clients are the French Ministries of the Interior, Justice, Economy and Finance, as well as companies such as Total, Axa, Veolia, SNCF and RTE.[9] The *Safe City* project uses Deveryware's 'Notico-Safe' software, developed through European research and development projects, the aim of which is to simultaneously alert citizens on their smartphones in the event of danger or natural disaster. In addition to this functionality, Deveryware has designed a new generation 112 emergency call, allowing citizens to be connected to a nearby rescue centre (CTA). They are two systems which, in order to function, must geolocate citizens from their smartphones.

In Marseille, the Engie Ineo company, which has since become Engie Solution, is in charge of the "Big Data Observatory for Public Tranquillity" project. The video surveillance market leader, a subsidiary of the Engie group, is also a stakeholder in the *Safe City* Nice project.

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

The development of the *Safe City* of Nice poses several problems for the political opposition and city activists. They denounce the opacity of the project, even though it directly impacts the citizens of Nice. In the partnership agreement signed between the city of Nice and the consortium of companies, the latter worry about a potential "paradigm shift and policies that would put security on the back burner". For the project to work, the mayor must continue to make safety a priority. They therefore play on the unconscious 'fears' of its population, by defining its city "under the prism of insecurity, as places of social disorganisation," as defined by Myrtille Picaud,[10] researcher associated with the "Cities and digital" and chair of the Sciences Po Urban School and the Center for European Studies and Comparative Politics (CEE).

Some members of the Nice opposition are worried about this security discourse, such as former socialist city councillor Paul Cuturello, who tried to question the municipality when the partnership agreement was adopted. "It's very disturbing. Public safety takes a back seat behind the commercial ambitions of the companies in the consortium."[11]

[9] Deveryware website, "Deveryware: Who are we?" https://www.gicat.com/membre/deveryware/

[10] Myrtille Picaud (2020), The Conversation France, "Fear of the city: the 'safe cities' market" https://theconversation.com/peur-sur-la-ville-le-marche-des-safe-cities-138313

[11] Clément Pouré et Clément le Foll (2020), Les Jours, "Nice, le « little brother » de Thales" https://lesjours.fr/obsessions/thales-surveillance/ep1-nice-safe-city/

Other politicians are concerned that this project will lead to the mass surveillance of citizens and that it may be hijacked to spy on activists, activists and political opponents. From 2018, a few months before the implementation of the General Data Protection Regulation, a European regulation which reinforces the constraints of collection and processing, the National Commission for Information Technology and Freedoms, responsible for ensuring the protection of personal data contained in the files and computer or paper processing, was worried about the development of smart cities, whose safety is the security version . *"The possibility of anonymity in the city is fading,"* wrote the National Commission for Information Technology and Freedoms in a press release .[12]

The local branch of the Human Rights League, an association for the defence of French individual freedoms founded in 1898, shares this observation, and is concerned that the city of Nice keeps the data collected and thus replaces the services of the national police. "The role of a municipality is not to develop a general intelligence service, which, inevitably, would end up serving the partisan interests of the small team in power".[13] In a *Safe City*, the detection of "abnormal behaviours" is defined by algorithms and is therefore biased, through those who created them, raising the risk that certain populations or people will be stigmatised.

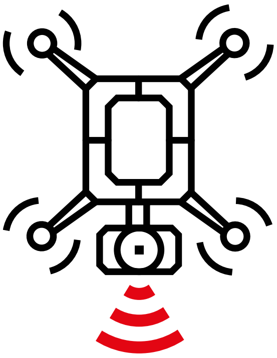
The La Quadrature du Net association speaks of a *"militarisation of public space,"* with private companies like Thales, whose historical activity is to build systems which are then used in battlefields and wars, who have adapted their technologies over time and are now deploying them in the public space. With the *Safe City*, the movements and personal data of a citizen can be collected and analysed by algorithms, with the simple aim of anticipating their future behaviour, such as travel, meetings and purchases. In this security vision of the city developed in Nice, the security of the population, competence of the municipality itself, is subcontracted to a private company. *"In the administration of our public spaces, there are logics of the market, of competition, of standardisation which are totally foreign to it and which can only lead to drifts, the first being to make them experimental grounds for these start-ups which can develop their surveillance tools with complete impunity,"* explains researcher Myrtille Picaud.[14]

[12] Guénaël Pépin (2017), NextImpact, "Smart city: the CNIL paints a grim picture for individual freedoms". https://www.nextinpact.com/article/27434/105426-smart-city-cnil-dresse-tableau-sombre-pour-libertes-individuelles

[13] Website of the Human Rights League of Nice (2018), "Observation n° 7, Response to the mayor of nice: 'safe city' or 'allo mairie'?" https://site.ldh-france.org/nice/2018/08/27/safe-city-criminogene/

[14] Clément Pouré & Clément le Foll (2020), Lesjours.fr, "The security thought colonizes the management of the city" https://lesjours.fr/obsessions/thales-surveillance/ep4-interview-picaud-castagnino-surveillance/

TREND 2:



WITH THE PANDEMIC, **SURVEILLANCE DRONES** ARE INVADING PUBLIC SPACE

It was in Istres, a city of 43,000 inhabitants located in the south-east of the country, a 55 kilometers from Marseille, that municipal police drones first flew over French skies. Only the national police and the Gendarmerie had so far used them in the context of the eviction from the defended area of Notre-Dame-Des-Landes.[15]

In April 2018, Mayor François Bernardini (left) announced that he was equipping his municipal police (composed of 80 people) with two drones. Equipped with Ultra HD cameras recording 30 images per second, these drones broadcast, with a few milliseconds of delay, the images filmed on the screens of the city's CSU. "They offer an additional means in the service of daily security, but also for the surveillance of forest massifs in the summer or the many parties or festivals that

[15] Pascal Simon (2018), Ouest France, "Notre-Dame-des-Landes: How the Gendarmes used drones" https://www.ouest-france.fr/pays-de-la-loire/notre-dame-des-landes-44130/notre-dame-des-landes-comment-les-gendarmes-ont-utilise-les-drones-5894651

we organize outdoors. It is a technology of the future, everyone will come to it,"[16] said François Bernardini.

The COVID-19 pandemic has served as justification for mayors across France who have equipped their municipal police with drones. The Interior Ministry is responsible for providing those used by the Gendarmerie and the national police. The objective of this drone surveillance is to ensure compliance with the confinement. In Lyon,[17] the national police and the departmental public security directorate used drones to enforce containment measures. "National Police. All movement is prohibited. Go home, said the aircraft at the sight of food deliverers, who continued to work and talk while waiting for the preparation of food orders.

Helicopters and drones also flew over the coastlines, to monitor walkers strolling along the beaches or to access areas that the police could not reach on foot. Near Montpellier, two drones were used to monitor the beaches of Palavas and Carnon. However, they also allow the police to monitor working-class neighbourhoods. "The purpose of the drones is to do reconnaissance, to find out if we have anchor points in the neighbourhoods, and to avoid sending a team into an ambush. There are pockets of resistance. Individuals who are still in the same place and who will be fined four or five times will be sanctioned for deliberately endangering the lives of others and they may be placed in police custody," explains Yannick Blouin, the departmental director of public security in Hérault.[18]

In Cannes,[19] also in the south-east of France, Mayor David Lisnard, who deployed all kinds of gadgets in the hope that they would help curb the pandemic, sprayed bleach with a drone in an attempt to disinfect one of the city's markets. Paris was not spared. Many drones monitored the French capital during the first confinement. In total, several dozen cities were scrutinised by drones during the first French confinement from March 17 to May 10, 2020.

[16] Marc Leras (2018), Le Parisien, "Istres: the municipal police acquire surveillance drones, a first" https://www.leparisien.fr/faits-divers/istres-la-police-municipale-se-dote-de-drones-de-surveillance-une-premiere-11-04-2018-7659057.php

[17] Catherine Lagrange (2020), Le Parisien, "National Police. Go home: in Lyon, drones enforce confinement" https://www.leparisien.fr/societe/police-nationale-rentrez-chez-vous-a-lyon-les-drones-font-respecter-le-confinement-10-04-2020-8297343.php

[18] Joane Mériot (2020), France 3 Occitanie, "Coronavirus: helicopters and drones to enforce confinement in Hérault" https://france3-regions.francetvinfo.fr/occitanie/herault/coronavirus-helicopteres-drones-faire-respecter-confinement-herault-1804528.html

[19] Alexandre Carini (2020), Nice Matin, "Cannes is experimenting with a drone to disinfect the Bocca market" https://www.nicematin.com/vie-locale/cannes-experimente-un-drone-pour-desinfecter-le-marche-de-la-bocca-493890

COVID-19 is not the only reason given for the spread of drones: the so-called migration crisis is another. For several years, French border surveillance has sometimes been carried out using drones, especially with that of Belgium.[20] More recently, the British Army used a drone to fly over the English Channel, which separates the United Kingdom from France.[21] This is in the line of sight of the border city of Calais, a French city where migratory pressure is the strongest and where refugees are harassed and live in inhuman conditions. In April 2020, the Ministry of the Interior launched a call for tenders for the acquisition of 650[22] drones for the national Gendarmerie, national police and civil security, i.e. double the number of drones currently in the hands of law enforcement.

COMPANIES INVOLVED

DJI is a Chinese company, a world leader in the manufacture of recreational, professional and corporate drones, created in 2006 by Frank Wang. The Shenzhen-based company was recently banned in the United States because the government believed their use poses a risk of espionage by the Chinese regime.[23] Through the French distributor Flying Eyes, around fifteen DJI Mavic Enterprise models[24] were used by the Paris police headquarters during the confinement, acquired on March 18, 2020, as part of a framework agreement for a public contract.

Parrot, a French company created in 1994, and specialised in digital and connected objects, was selected on January 12, 2021 by the French Ministry of the Armed Forces, to supply 300 micro-drones, to be delivered from June 2021.[25] They will be used for reconnaissance and intelligence missions. Able to fly for thirty minutes , they weigh less than 500 grams and can fly day and night. They are "able to detect human-sized targets with great precision, up to two kilometres away, are particularly discreet and even inaudible over 130 metres, and can be implemented in less than a minute," explains the Ministry of Defense.

[20] Bruno Susset (2018), Est Républicain, "Belgian drones to monitor the border between France and Belgium" https://www.estrepublicain.fr/le-mag/2018/12/07/des-drones-douaniers

[21] George Allison, 2020, UK Defense Journal, "Watchkeeper drone carries out border patrol over the English Channel" https://ukdefencejournal.org.uk/watchkeeper-drone-carries-out-border-patrol-over-the-english-channel/

[22] Fabien Leboucq (2020), Liberation, "Why has the Interior Ministry just ordered drones?" https://www.liberation.fr/checknews/2020/04/15/pourquoi-le-ministere-de-l-interieur-vient-il-de-commander-des-drones_1785166/

[23] BBC (2020), "Chinese drone and chip makers added to US banned list" https://www.bbc.com/news/technology-55367163

[24] DJI website, " Mavic 2 Enterprise series" https://www.dji.com/fr/mavic-2-enterprisehttps://www.dji.com/fr/mavic-2-enterpris

[25] French Ministry of Defense website, "The Ministry of the Armed Forces orders new reconnaissance and intelligence micro-drones" https://www.defense.gouv.fr/actualites/articles/le-ministere-des-armees-commande-de-nouveaux-micro-drones-de-reconnaissance-et-de-renseignement

The defence and aerospace giant Thales, of which the French State and the company Dassault Aviation are the majority shareholders, is involved in the construction of the Watchkeeper WK 450 drone,[26] used in September 2020 by the British army in a surveillance operation of the British and French borders. To design this drone, initially deployed in Afghanistan on military grounds by the British military, Thales teamed up with the Israeli company Elbit.

Founded in 1953, the company made a name for itself by developing the Hermes drone model. A few months ago, Canada spent more than 36 million USD to obtain a Hermes 900 StarLiner,[27] which will be responsible for carrying out maritime surveillance. Elbit is also the source of much controversy. In 2018, US investigative media *The Intercept* revealed that a Hermes 450 drone was used in 2014 by Israel Defense Forces to bomb the Gaza Strip in Palestine, killing four children[28].

Drone Watchkeeper WK 450, coproduced by Thales and Elbit.

[26] Thales Group Website, “Drone tactique Watchkeeper” https://www.thalesgroup.com/fr/worldwide/defense/drone-tactique-watchkeeper

[27] Levon Sevunts (2020), RCINET, “Canada buys Israeli drone for Arctic maritime surveillance” https://www.rcinet.ca/eye-on-the-arctic/2020/12/22/canada-buys-israeli-drone-for-arctic-maritime-surveillance/

[28] Secret Israeli Report Reveals Armed Drone Killed Four Boys Playing on Gaza Beach in 2014 https://theintercept.com/2018/08/11/israel-palestine-drone-strike-operation-protective-edge/

IMPACT ON SOCIAL MOVEMENTS

Since the start of the pandemic, drones have been used to monitor at least five Parisian demonstrations and have been used to arrest several health union activists who carried out non-violent action on July 14, 2020.[29] The extension of several intelligence files (see part V), the project to legalise drone surveillance via the global security bill and the proliferation of facial recognition tools are of particular concern to civil liberties associations, who see it as a tool that can be misused to monitor activists.

The use of drones by law enforcement immediately sparked a rebellion from civil liberties groups and lawyers. At issue was the legal vagueness that accompanies their use.

The legal framework for the use of drones is particularly unstable. It is defined by the decree of December 17, 2015,[30] which sets the conditions for the use of "airspace by aircraft traveling without anyone on board," and which provides that each drone flight must be declared at the prefecture at least five working days before the flight. However, this decree exempts the national police and the Gendarmerie from any declaration of theft from the moment *"the circumstances of the mission and the requirements of public order and security justify it."*

In the case of this use, the police can use their drone without citizens knowing when they are being filmed, if the images are transmitted or recorded, and the data is stored. An opacity that raises concerns about breaches of privacy and respect for personal data. Mainly initially deployed to fly over major highways, drones have been used for several months to monitor protests.

A lawyer at the Paris Bar, Thierry Vallat, a specialist in digital law, points to an increasingly invasive use of drones as these technologies have matured. *"From the surveillance of forest, their use has extended to demonstrations of the yellow vests and sporting events".*[31]

Faced with this lack of a legal framework, the Council of State, the highest French administrative court, which had been applied by the association for the defence of public freedoms, La Quadrature du Net, and the League of Human Rights, on 18 May 2020 ordered the State to stop *"without delay"* the use of drones in Paris to monitor compliance with the rules of deconfinement.[32] The Council of State estimated that drones could fly at distances that allowed the identification of

[29] Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

[30] Légifrance, "Order of 17 December 2015 relating to the use of airspace by aircraft traveling without anyone on board" https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031679868/

[31] Clément Pouré & Clément Le Foll (2020), Médiapart, "With containment, drones are intruding into public space" https://www.mediapart.fr/journal/france/250420/avec-le-confinement-les-drones-s-immiscent-dans-l-espace-public

[32] Council of State (2020), "Decision on drone surveillance in the context of deconfinement" https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

individuals. *"Under these conditions,"* notes the Council of State, *"the data likely to be collected by the disputed processing must be regarded as being of a personal nature."* The court demands that the state cease *"without delay, to carry out surveillance measures by drone"* as long as a regulatory text, according to the opinion of the National Commission for Informatics and Freedoms, the French digital Gendarme, does not clarify their use.

Despite this decision, whose field of action was to cover the whole of France, the security forces continued to deploy drones to film the various demonstrations, raising fears of an attack on the freedom to demonstrate. *"The collection of information [note - by means of drones] on the participants in an action of the General Confederation of Labour (CGT) or a demonstration organised by a religious movement is for us an unjustified processing of sensitive data,"* recalls Martin Drago, lawyer at La Quadrature du Net.[33]

While the Paris police headquarters justified the use of drones by resorting to software capable of blurring the silhouettes captured by the images of the drones, and thus anonymising the data, a Mediapart survey explained in November that this software does not was only effective in 70% of cases.[34]

At the end of December, the Council of State this time ordered the Paris police chief Didier Lallement to stop using drones to monitor the demonstrations, a second victory for the defenders of civil liberties, particularly La Quadrature du Net, at the origin of the appeal.[35] It was a snub for the French government, which plans to expand the use of drones through article 22 of the comprehensive security bill, which is due to go back to the National Assembly in early 2021.

From January to June 2018, up to "six or seven drones" per day were deployed to monitor the ZAD of Notre Dame des Landes, for example.[36] On some days, six to seven drones flew over the area, as did police helicopters. *"It facilitates the tactical support of ground units. This allows us to observe very closely, and discretely, what is happening behind a hedge, to spot individuals preparing ammunition…"*[37] explained Lieutenant-Colonel Henri Dulong de Rosnay, Commander of the group of the Gendarmerie Air Force in west France.

[33] Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

[34] Clément Pouré & Clément le Foll (2020), Médiapart, "Drones: when it comes to blurring the demonstrators, the police are less careful" https://www.mediapart.fr/journal/france/181120/drones-quand-il-s-agit-de-flouter-les-manifestants-la-police-moins-regardante

[35] La Quadrature du Net (2020), "Interdiction des drones victoire totale contre le gouvernement" https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/

[36] Pascal Simon (2018), Ouest France, "Notre-Dame-des-Landes: How the Gendarmes used drones" https://www.ouest-france.fr/pays-de-la-loire/notre-dame-des-landes-44130/notre-dame-des-landes-comment-les-gendarmes-ont-utilise-les-drones-5894651

[37] Idem

Police drones and the national Gendarmerie have also been regularly used to monitor demonstrations, including the yellow vests movement. In an article published by Mediapart, three activists from the Inter-Urgences collective participating in a march organised at the call of caregivers unions and supported by the yellow vests, testified that they were identified thanks to drones after having deployed a banner accusing French President Emmanuel Macron of "suffocating the hospital". These are two concrete examples which show how drones can allow the police to monitor activists in places they cannot go, but also to stop activists by exploiting the filmed images.

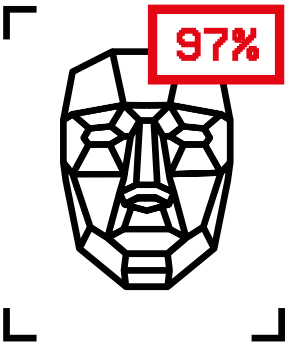
Since the start of the pandemic, and despite a first judgment by the Council of State pointing out the absence of a legal framework surrounding the use of drones in the context of deconfinement, drones have been used to monitor at least five Parisian demonstrations and were used to arrest several health union activists who carried out non-violent action on July 14, 2020.[38]

The extension of several intelligence files (see part V), the project to legalise drone surveillance via the global security bill, and the proliferation of facial recognition tools are of particular concern to civil liberties associations, which see it as a tool, can be led astray to monitor activists.

At the beginning of January, the French National Freedom and Information Commission sanctioned the use of drones by the French government. In its opinion, the authority explains that the blurring mechanism developed by the Ministry of the Interior was only put in place in August, when many flights had already been carried out. *"Moreover, this mechanism cannot be executed directly by the drone. Images containing personal data are therefore collected, transmitted and processed by the Ministry of the Interior before this blurring system is applied,"* the CNIL said.

[38] Clément Pouré & Clément le Foll (2020), Médiapart, "Taking advantage of legal vagueness, police drones are still buzzing" https://www.mediapart.fr/journal/france/261020/profitant-du-flou-juridique-les-drones-policiers-bourdonnent-toujours

TREND 3:



FACIAL RECOGNITION AND BIOMETRICS

The use of real-time facial recognition in public spaces is inseparable from a city in the south of France which is at the forefront of surveillance technologies: Nice. In February 2019, the city's carnival, which lasts for two days, was the scene of the first facial recognition experiment in a public space in France. Several cameras placed at one of the entrances to the carnival were responsible for identifying 50 volunteers. Following this experiment, the city of Nice was delighted that the algorithm was able to recognise these 50 individuals. The national information and freedoms commission is more reserved about it and considers that the experimental report transmitted by Nice was incomplete and did not allow conclusions to be drawn on its success.[39]

In December 2018, still in the south of France, the council of the South region (formerly PACA) authorised an experiment to install facial recognition gates in two

[39] Le Journal du Net (2019), "Facial recognition experimentation: Nice delighted, Cnil skeptical" https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/

high schools: the Eucalyptus high school in Nice and the Ampère high school in Marseille.[40]

For several years, the Parisian airports of Roissy Charles de Gaulle and Orly, frequented by 76.2 million and 31.9 million travellers respectively in 2019, have been equipped with facial recognition gates, called SAS PARAFE (for rapid automated crossing of external borders).[41] These devices are also installed at Marseille-Provence, Lyon Saint-Exupéry and Nice airports, as well as at the railway stations Gare du Nord in Paris and Saint-Pancras in London. They are also deployed at the Eurotunnel for coaches.

A few months ago, the French State also wanted to bring facial recognition into the daily lives of French people, by launching ALICEM, a smartphone application developed by the Ministry of the Interior and the French National Agency for Secured Documents (ANTS). Its goal is to enable individuals to prove their identity on the Internet, using their smartphone and passport or residence permit, and to access various administrative procedures.

The proposed law regulating the use of facial recognition in French public spaces is under debate at political level. Among those who are in favour of its application, is the mayor of Nice, Christian Estrosi, who is behind the first experiment on French soil. For French parliamentarians, the 2024 Olympic Games, which will take place in Paris, appear to be the perfect event to legislate or launch a life-size experiment in facial recognition.[42]

While real-time facial recognition is still banned in France, it is already a reality for law enforcement. Since 2011, it has had software allowing it to compare images from video surveillance or social networks with those contained in the TAJ file (the processing of criminal records) which includes more than 8 million photographs of French residents. In the first half of 2020, more than 200,000 requests had been made concerning this file, according to the Next Impact website[43].

[40] Quadrature du Net website (2019), "Facial recognition in high schools: an impossible debate?" https://www.laquadrature.net/2019/10/15/reconnaissance-faciale-dans-les-lycees-debat-impossible/

[41] Website of the Ministry of the Interior, "PARAFE: passing border controls faster" https://www.interieur.gouv.fr/Actualites/Infos-pratiques/PARAFE-passer-les-controles-aux-frontieres-plus-rapidement

[42] Clément Pouré and Clément Le Foll (2020), Lesjours.fr, "Thales is involved in your face" https://lesjours.fr/obsessions/thales-surveillance/ep5-reconnaissance-faciale/

[43] Pierre Januel (2020), NextImpact, "Police: the massive use of facial recognition is confirmed" https://www.nextinpact.com/article/44242/police-emploi-massive-reconnaissance-faciale-se-confirme

COMPANIES INVOLVED

Thales Digital Identity and Security is the subsidiary of the Thales company, dedicated to biometrics. This entity was born in 2019, when Thales concluded the acquisition of the Franco-Dutch biometrics specialist Gemalto.[44] With this purchase, Thales acquired a wide range of cutting-edge technologies and is returning to a market that it left in 2017 by selling its identity management activity[45] to IN Groupe (the Imprimerie Nationale) such as civil status data, and the production of secure documents, among others. Two years later, with the acquisition of Gemalto, Thales has asserted itself as one of the world leaders in biometrics.

Through Gemalto, Thales took over the management of SAS PARAFE (to pass border controls more quickly). Originally based on the correspondence of the biometric fingerprint, the new PARAFE system, implemented in 2018, uses security gates. Placed in airports, they use data from biometric passports and facial recognition. While passing through the airport, a European Union national scans his or her passport for the first time on a reader, which opens an airlock, into which the individual steps. Their face is subjected to facial recognition and the second door opens after a 10 to 15 second delay. In 2017, Gemalto announced the launch of a solution called 'Fly to Gate',[46] where an individual could be tracked from their home to their flight's boarding gate, using facial recognition.

Thales is also involved in ALICEM, a facial recognition system developed by the French Ministry of the Interior in 2019. This certified online authentication device on mobile devices has been in the test phase since June 2019 at ANTS. It comes in the form of an Android mobile application, which will connect to public services such as taxes, health insurance or social security through authentication by facial recognition of facial features. Scheduled for 2019, the launch of ALICEM has been delayed and is expected to begin in 2022.

In early November 2020, Thales announced its 'Identity Verification Suite',[47] a project still at the pilot stage, aimed at service providers who wish to verify the identity of their customers remotely. It relies on biometric verification via a selfie taken with a smartphone.

[44] Thales group website, "Thales and Gemalto create a world leader in digital security"
https://www.thalesgroup.com/fr/thales-et-gemalto-creent-un-leader-mondial-de-la-securite-digitale

[45] Ingroup website (2017), "Thales signs an agreement with the Imprimerie Nationale Group on the sale of its identity management activity"
https://www.ingroupe.com/newsroom/thales-signe-un-accord-avec-le-groupe-imprimerie-nationale-sur-la-cession-de-son-activite-de-gestion-d-identite

[46] Thales group website, "Border control"
https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/controle-aux-frontieres

[47] Thales group website, "Thales launches its new identity verification offer, a secure biometrics-based solution for remote customer enrollment"
https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-lance-sa-nouvelle-offre-verification-didentite-une-solution

Anyvision is an Israeli company founded in 2015 specialising in the cybersecurity and facial recognition technology sector. Its founders included academic staff and cybersecurity experts. Its facial recognition software 'Better tomorrow' – which claims to have less than 0.1% of errors – was coupled with surveillance cameras in Nice during the carnival, for the first facial recognition experiment in public space in France .

Cisco is an American IT company based in California. Founded in 1984, it was originally specialised in network hardware before gradually moving towards artificial intelligence. The company was selected in 2019 to couple facial recognition software to the cameras of two high schools in Marseille and Nice. A digital file containing the name and photo of the student would have been created by the establishment, to generate a QR code that can be displayed on the phone. Each time they entered high school, the students would have scanned this QR code on a dedicated gantry, equipped with a camera that would have scanned their face and compared it with the one held in the file[48]. The project was finally abandoned.

Idemia is a French company created in 2017 from the merger of Morpho, the identity and security branch of the company Safran, specialising in aeronautics and space, and the company Oberthur Technologies. The company is now specialised in biometric identity and collaborates with Thales and In Groupe on the development of SAS Parafe. Idemia is also working on the construction of databases essential for the proper functioning of facial recognition.

A few months ago, along with another French company, Sopra Steria,[49] the company won the contract awarded by the European Union to create a biometric database for border controls in the Schengen area. Scheduled for 2022, it will integrate the fingerprints and portraits of more than 400 million third-country nationals. Idemia is currently working on a new facial recognition software called Augmented Vision. "This software scans video surveillance images in real time and post-event. After an attack in the metro, for example, it can find on the images a face appearing in a pre-established list of interest, reconstruct trajectories and interactions between people," explains Vincent Bouatou, innovation director of the identity and public security department of Idemia.[50]

[48] Romain Baheux (2019), Le Parisien, "Facial recognition tested in high schools"
https://www.leparisien.fr/societe/video-dans-les-lycees-et-maintenant-place-a-la-reconnaissance-faciale-04-02-2019-8004192.php

[49] Sopra Steria website, "IDEMIA and Sopra Steria chosen by the French Ministry of the Interior for the development of a centralized border control system"
https://www.soprasteria.fr/media/communiques/details/idemia-et-sopra-steria-choisis-par-le-ministere-de-l-interieur-fran%C3%A7ais

[50] Marion Garreau (2020), L'Usine Nouvelle, "How the French Idemia exploits the biometric vein"
https://www.usinenouvelle.com/editorial/comment-le-francais-idemia-exploite-le-filon-biometrique.N1026034

The processing of the TAJ file is done using tools developed in-house by the French law enforcement agencies, but also includes private partnerships. Since 2011[51] the police have used the facial recognition software 'Facevacs Dbscan', marketed by the German company Cognitec, which works with many integrators such as Indemia and Atos.

IMPACT ON PUBLIC FREEDOM

February 27, 2021, Montreuil (93), France.[52] Le Marbré, a city squat, is organising an evening of support for activists imprisoned in Meaux following the fire at an administrative detention centre last January. The police come to expel them. The activists resisted but are finally arrested. Several of them refuse to give their identities. Law enforcement takes pictures of them and identifies them using facial recognition software. *"Some people have been identified after refusing to disclose their identity,"* write the activists, *"and after the cops have photographed them and compared their photos via a facial recognition system, two of those initially inside have been taken into police custody."*

Through the government's ALICEM project, which aims to access administrative services through facial recognition, or the recent launch by Thales of its 'Identity Verification Suite', aimed at service providers who wish to verify the identity of their clients and remote customers, several observers see a desire to bring about acceptance of facial recognition by immersing it in the daily lives of the population. *"It is by deploying biometrics presented as harmless that we create consent,"*[53] explains Olivier Tesquet, specialised journalist specialized on surveillance issues.

A few months ago, the association La Quadrature du Net, before the Council of State,[54] the highest French administrative court, attacked the provisions of the code of criminal procedure which authorise the police to use facial recognition to identify data subjects in the TAJ. This file contains the photographs of the faces of any person 'implicated' in a police investigation, whether convicted or cleared. The TAJ now contains, according to a parliamentary report and the CNIL, 19 million files and 8 million face photographs. "Biometric surveillance is exceptionally invasive and dehumanising. It allows invisible, permanent and generalised control of the public space. It turns us into a society of suspects. It gives our body a function of constant tracer, reducing it to a technical object of identification. It

[51] Gabriel Thierry (2019), l'Essor, "Why the legal challenge of facial recognition could make pschitt" https://lessor.org/a-la-une/pourquoi-contestation-judiciaire-reconnaissance-faciale-pourrait-faire-pschittt/

[52] Indymedia Nantes, "Montreuil (93): expulsion from Marbré" https://nantes.indymedia.org/articles/54990

[53] Clément Pouré & Clément Le Foll (2020), Lesjours.fr, "Thales is involved in your face" https://lesjours.fr/obsessions/thales-surveillance/ep5-reconnaissance-faciale/

[54] Quadrature du Net website (2020), "We are attacking facial recognition in TAJ" https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/

abolishes anonymity," the statement said.

As the association explains, one of the risks that hovers around the use of facial recognition, beyond the fact that any individual will no longer be able to be 'anonymous' when cameras identify them, is on the freedom to demonstrate. The proliferation of police files "is serious enough to deter a large part of the population from exercising their right to demonstrate." The use of facial recognition in the demonstrations would have a perverse effect on the demonstrators, who would feel oversight in the exercise of this right. "The ability to be part of an anonymous crowd is what allows many people to participate in peaceful protests and feel safe," Amnesty International said.[55]

[55] Amnesty International website (2020), "As protests continue around the world, facial recognition technologies must be banned" https://www.amnesty.org/fr/latest/news/2020/06/usa-facial-recognition-ban/

TREND 4:

INTELLIGENT VIDEO SURVEILLANCE SYSTEMS ON THE ASSAULT OF CITIZENS

In her book, *The Safe Eye: Myths and realities of video surveillance*, sociologist Elodie Lemaire recounts in particular the daily life of video operators, stationed in an urban supervision centre and responsible for scrutinising the cameras and sometimes taking control of them. It depicts an atypical profession, both in terms of its status and the role of operators, some of whom avoid the slightest offense, while others are content to watch and communicate on the fluidity of road traffic. *"In addition, if the practices of the agents stationed behind the cameras differ, what they have in common is that they do not know the real impact of video surveillance, both in terms of prevention (deterring action) and that of repression (clarifying legal cases),"* explains the sociologist.[56]

After installing cameras in hundreds of French municipalities, industry manufacturers are now betting on these potential flaws in video operators to try to sell

[56] CNIL website (2019), Elodie Lemaire: "Video surveillance is not ideal proof" https://linc.cnil.fr/fr/elodie-lemaire-la-videosurveillance-nest-pas-une-test-ideale

artificial intelligence software. Coupled with the cameras already installed, they allow you to focus on certain elements: cars, colours, a silhouette or even to condense several hours of videos into a few seconds. Computer-assisted processing is close to facial recognition but which does not use biometric data.

This was a choice made by the city of Roubaix,[57] in the north of France. In June 2020, the city inaugurated its new police station. It brought together municipal police and an urban supervision centre, which centralises all the images from the city's 123 CCTV cameras. The artificial intelligence software makes it possible to perform video tagging, zoom in on individuals and monitor streets, metro exits or carparks in real time. Some of the largest cities in France, such as Lyon or Marseille (even if the project is subject to an audit by the municipality) have also chosen to develop intelligent video surveillance. This technology has also been used since 2014 by the national police in the context of criminal investigations.[58]

COMPANIES INVOLVED

Briefcam is an Israeli company specialising in the production of video surveillance image analysis software. It was founded in 2008 on the basis of VIDEO SYNOPSIS technology, developed by Shmuel Peleg, researcher at the Hebrew University of Jerusalem. Briefcam is a subsidiary of the Japanese company Canon, which owns other companies in the video surveillance industry such as Axis and Milestones.

Coupled with a camera, the VIDEO synopsis software allows the video operator to apply numerous filters to the images filmed. It is possible to focus on two-wheeled vehicles, vans, trains or buses, but also to identify certain types of clothing by colour or by the length of their sleeves. The software also makes it possible to locate objects and people according to their size, trajectory and to carry out searches by license plate. In 2020, the company claims to be present in 30 French cities, Roubaix, Vannes, Nice and Nîmes.

Hikvision is a Chinese company specializing in the design of video surveillance and intelligent software founded in 2001. The company is one of the world market leaders with a turnover of 41.9 billion yuan in 2017, or about 5 billion euros. In addition to a dozen different cameras, Hikvision markets a series of products

[57] Anne-Sophie Hourdeaux (2020), Actu.fr, "Video surveillance in Roubaix: cutting-edge technologies to keep an eye on the city" https://actu.fr/hauts-de-france/roubaix_59512/video-surveillance-roubaix-technologies-pointe-garder-loeil-sur-ville_30822291.html

[58] Biometric Update (2016), "French National Police using Safran's Morpho Video Investigator solution" https://www.biometricupdate.com/201612/french-national-police-using-safrans-morpho-video-investigator-solution

based on deep learning, making it possible to focus on certain elements of video surveillance images.[59]

The company claims to equip 300 French municipalities. *"We are able to recognise the approach of an individual at 200 metres at night, distinguishing them from a stray animal or a fallen branch, for example,"* explained its CEO, Jean-Baptiste Ducatez.[60]

Huawei is a Chinese company founded in 1987 by Ren Zhengfei, specialising in the information and communication technology sector. In February 2017, Huawei offered the city of Valenciennes 217 new generation cameras and a surveillance centre. In addition to being able to do facial recognition – which the municipality says it does not use – they are equipped with new technologies developed by Huawei: HD zoom, night vision and in the rain, intelligent image processing with detection of crowd movements, abandoned objects, unusual situations.[61]

The French company EVITECH was founded at the end of the 2002 following a project by the Ministry of Defence, aimed at preventing events such as the hostage-taking of the Moscow theatre on October 26, 2002. It specialises in intelligent video surveillance software. Its 'Jaguar' solution has, since 2010, been installed on 70 cameras in the port of Lyon. It allows the counting of vehicles, the detection of vehicles at a standstill, going in the wrong direction speeding.[62] More recently, the 'Lynx' software has enabled the city of Lyon[63] to count the evolution of the number of people present on the Place des Terreaux during the Festival of Lights. A similar device is deployed in the municipality of Hurepoix.[64]

[59] Hikvision Website, "Hikvision CCTV systems for perimeter protection" https://www.hikvision.com/en/solutions/solutions-by-application/perimeter-protection/

[60] Jordan Pouille (2020), La Vie, "How" intelligent "video surveillance is needed in French cities" https://www.lavie.fr/actualite/comment-la-videosurveillance-intelligente-simpose-dans-les-villes-francaises-2816.php

[61] Huawei website (2017), "Valenciennes inaugurates a new video protection system and is part of a" smart city "approach with Huawei" https://e.huawei.com/fr/news/fr/2017/170213_valenciennes_safe_city

[62] Evitech website (2011), "EVITECH experience feedback in urban video surveillance" https://www.evitech.com/fr/component/content/article/20-blog/references/31-retour-experience-evitech-video-surveillance-urbaine

[63] Evitech website (2018), "Counting at the festival of lights in Lyon" https://www.evitech.com/fr/component/content/article/20-blog/references/326-comptage-a-la-fete-des-lumieres-a-lyon?Itemid=136

[64] Evitech website (2019), "Revitalization of a city center" https://www.evitech.com/fr/component/content/article/20-blog/references/349-revitalisation-d-un-centre-ville?Itemid=136

IMPACT ON SOCIAL MOVEMENTS AND OTHER POLITICAL ACTORS

This software, which is coupled with video surveillance, has a concrete impact on video operators, but also on individuals who are observed in a public space by these cameras.

In Le Carnet,[65] in Loire-Atlantique, environmental activists fighting against the concreting of a natural site discovered that cameras had been camouflaged to be able to spy on them. Camouflaged in tree stumps or false pebbles, these four cameras filmed continuously and were connected, via buried cables, to large hidden batteries and modems, allowing images to be sent directly to a remote station. *"The mention of 'Allwan', visible on some of the images found, or on a label on a camera, strongly suggests that it is equipment provided by the company Allwan Security, located near Angers (Maine-et-Loire), specialised in video equipment. This company only deals with professionals, and counts law enforcement among its important clients,"* the article explains.

In May 2020,[66] the police of Millau, in Aveyron, used the city's CCTV cameras to confirm the identity of demonstrators who participated in two undeclared demonstrations in the prefecture to denounce the management of the COVID-19 crisis and support public services and the health system. About ten days later, some activists confided that they had received a fine of €135 for *"a prohibited assembly on the public highway in a territorial district where the state of health emergency has been declared."* A verbalisation made possible by the exploitation by the police of the video surveillance images. *"The videos are not supposed to be used to verbalise this type of offense,"* points out Julien Brel, the lawyer at the Toulouse Bar.

Teacher-researcher at the IMT Atlantique engineering school, Florent Castagnino,[67] has devoted his thesis to surveillance systems within the SNCF. In a paper published in 2019, he describes how smart video surveillance displaces the work of video surveillance operators and redefines suspicion. *"The automation supposedly induced by artificial intelligence does not remove the work of operators but displaces it. This displacement of the object therefore must lead to the displacement of the empirical investigation towards the study of the work of computer scientists. The paper then shows how the latter must mathematically formalise part of the work of the operators in order to stabilise it in algorithmic rules. In this task of abstraction, they then make more or less implicit choices of what is 'suspect', and thus of what to 'watch out for'."*

[65] Héloïse Leussier (2020), Reporterre, "In Carnet, hidden and illegal cameras to monitor environmentalists
https://beta.reporterre.net/Au-Carnet-des-cameras-cachees-et-illegales-pour-surveiller-des-ecologistes

[66] Mélenn Gautier (2020), Liberation, "Can we be fined by video surveillance?"
https://www.liberation.fr/checknews/2020/08/03/peut-on-etre-verbalise-par-videosurveillance_1791447

[67] Florent Castagnino (2019), Science Po, "Making cameras 'smart': shifting the work of video surveillance operators and redefining suspicion"
https://www.sciencespo.fr/ecole-urbaine/sites/sciencespo.fr.ecole-urbaine/files/2019_05%20-%20Castagnino.pdf

In January 2020, two associations for the defence of individual freedoms, the Quadrature du Net and the League of Human Rights, filed an appeal before the administrative court of Marseille against a new intelligent video surveillance system set up by the city town hall of the city.

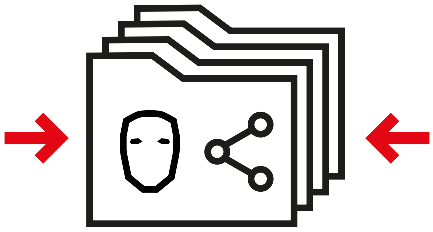
The associations believed that smart cameras captured biometric data, which is particularly sensitive and therefore protected, while the law does not allow them. *"Due to the very operation of the processing which leads to the alert, but also probably to the information transmitted by the alert, the contested decision authorises processing of biometric data – processing of behavioural characteristics, and also probably of physical and physiological characteristics, allowing a person to be uniquely identified."*[68]

La Quadrature du net and the Human Rights League were also concerned about a delegation of police powers to the company in charge of the project, SNEF, explaining that it was indicated in technical documents that the configuration of the algorithms would be produced by SNEF. "It will thus be up to the software solution of the private company to identify, categorise and generate alerts on certain events taking place on public roads," they worried.

One of the other impacts smart video surveillance could have is the ability to track the movements of a political opponent or activist through a network of cameras. The solution deployed by Briefcam allows vehicles or individuals to be filtered according to the colour of their clothing. An individual could thus be identified and then followed by all the cameras. In a video accessible on YouTube, a police officer in Hartford, United States, shows how the Briefcam software allowed him to identify the movements of individuals for several hours and thus realise that they were all taking the same direction, the drug dealer spot that he sought to dismantle.

[68] Olivier Tesquet (2020), Télérama, "Intelligent video surveillance is coming to Marseille, two associations are trying to have it suspended" https://www.telerama.fr/medias/deux-associations-attaquent-la-videosurveillance-intelligente-a-marseille

TREND 5:



THE PANDEMIC AS A PRETEXT FOR POLICE REGISTRATION

March 27, 2020. French Prime Minister Edouard Philippe announces confinement throughout the national territory. Those who do not respect it will be fined 135 euros. In the event of a repeat offense within two weeks, the offender can be fined 1,500 euros (reduced to 200 euros at the end of March). On April 15, the police and the National Gendarmerie carried out more than 12 million checks and issued 762,106 tickets.[69]

These violations are immediatly recorded in the Automated Control System (ACS). Also called Access to the Ticket File (ADOC), this police file was initially intended for traffic offenses. It is illegal to write down the penalties for non-compliance with containment. On April 9, Rennais lawyer Rémi Casette became aware of the legal loophole and obtained the release of one of these clients prosecuted for repeated non-compliance with confinement. All the current procedures for non-com-

[69] France Info (2020), "Coronavirus: 1,733 police custody for repeated containment violations since March 17"

pliance with confinement are weakened. We must act urgently. The government issues a decree on April 16 to rectify the situation, and extends, by the way, the SCA file with about thirty new offenses.

"Not only are the offenses concerned not very serious," points out La Quadrature du Net in an article published in November 2020[70], "but they are also numerous. You could therefore find yourself in this police file for having sold an Eiffel Tower model on the sly, for having cannabis on you, for dumping rubbish..."

In a parliamentary report dated 2009,[71] Delphine Batho and Jacques Alain Bénisti count 58 police files, 27% of which have not been the subject of any legal or regulatory authorisation or of a declaration to CNIL. A parliamentary report, this time dated October 2018,[72] reports a vast movement towards compliance and points out that the CNIL now considers that there is no longer any irregular implementation of important national reporting. Another observation made by parliamentarians: the multiplication of the number of data processing files, since they identify 106 files made available to the security forces.

French police files primarily consist of administrative files. They gather information on the entire French population, regardless of whether or not they have committed reprehensible acts. File of identity cards, driver's licenses: they are primarily intended for identification.

For several years now, a file has been of particular concern to associations for the defence of public freedom: the electronic security documents file, which groups together, in a centralised database, the digitised image of the face and fingerprints of all applicants for national identity cards and passports. This biometric data is kept for between 15 and 20 years. If the decree which allowed its creation clearly specifies that the police cannot access the fingerprints stored in the TES file, no formal legal limit prevents its use for facial recognition purposes and the forces can, via 'an application', access all data except fingerprints, according to the French Intelligence Research Center.[73]

Other police files, known as judicial files, concern people who have dealt with law enforcement. Aimed at "the collection and centralisation of information intended to fight against well-defined offenses,"[74] this file is equally concerns in stolen objects and vehicles (FOVeS), counterfeiting (FNFM) or even judicial authentication, such as the Automated Fingerprint File (FAED) or the National DNA File (FNAEG).

[70] Quadrature du Net website (2020), "Police registration: recourse against the misappropriation of the" automated control system file" https://www.laquadrature.net/2020/11/09/fichage-policier-recours-contre-le-detournement-du-fichier-du-systeme-de-controle-automatise/

[71] Delphine Batho and Alain Bénisti (2009), "Information report on police files" https://www.assemblee-nationale.fr/13/rap-info/i1548.asp

[72] Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces" https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#_Toc256000053

[73] Jean Marie-Cotteret (2017), "Police and intelligence files in France" https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf

[74] Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces" https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#_Toc256000053

Among them, the TAJ file, common to the police and the Gendarmerie, results from the merger of two older files and comprises more than 19 million files including 8 million photos (i.e. more than 10% of the French population).

It is not limited to people convicted by the courts, but centralises information of all the people who have been implicated in a legal case, and also the victims of offenses or the people under investigation for cause of disappearance. A report from the French Intelligence Research Center[75] describes the advantages of this new file compared to its predecessors. "The TAJ also presents changes in relation to the files it replaces: more categories of data subjects and new functionalities, such as tools for analysing and reconciling data, making it possible to search for common elements in different procedures or facial recognition from photographs of people."

The wanted persons file (RPF) has also been widely singled out. Created in 1969 and updated in 2017, this police file, common to the police and the National Gendarmerie and available for consultation on a tablet or on an on-board terminal, lists all the people "subject to a search or verification measure"[76]. An identification file, intended for the identification of persons and the collection of information, which includes in particular the 'S' files, for state security, that is to say "the people who can, because of their individual or collective activity, undermine state security and public security by resorting to or actively supporting violence, as well as those who maintain or have direct and non-fortuitous relations with these persons."[77] It is a broad definition, which includes as many people likely to belong to Islamist terrorist movements as militants and activists or even journalists.[78]

In December, a reform of all three of the files of the Prevention of attacks on public security (PASP), Information management and prevention of attacks on public security (GIPASP) and Administrative investigations related to public security files (EASP). Information linked to the general direction of the national police and the general direction of the national Gendarmerie made the representatives of public freedoms jump. They bring together extremely precise information (profession, physical addresses, email, photographs, public activities, behaviour, travel, etc.). These files identifying individuals for many reasons linked to the maintenance of order (illegal demonstrations, violence and damage linked to ideological disputes, hate speech, violence and vandalism during sporting events, etc.) were first extended to legal persons and 'groups'.

In other words, these files can now concern companies, associations, but also Facebook groups, activist spaces or simply public events (all comparable to

[75] Jean Marie-Cotteret (2017), "Police and intelligence files in France"
https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf

[76] CNIL website, "Wanted persons file"
https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees

[77] Didier Paris and Pierre Morel-à-L'Huissier (2018), "Information report on the files made available to the security forces"
https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/

[78] Marie-Pierre Hadad (2016), "How a journalist discovered that he was on file"
https://www.rtl.fr/actu/politique/comment-un-journaliste-a-decouvert-qu-il-etait-file-s-7786291210

groups). This reform also authorises the PASP and GIPASP to file persons "maintaining or having maintained direct and non-fortuitous relations" with the said 'group'. If the police deem it necessary, they can identify the people who participated in these groups (for example, a journalist present at the time). While these files hitherto excluded the registration of children, PASP and GIPASP could theoretically be used without age limit.

The same reform also extends the perimeter of the information collected, including lifestyle, online activities, posts published on social networks, among others. It opens the door to the generalised collection of data that the government has refused to formally exclude despite the request of the CNIL. Even more serious is that the decrees also authorise the collection of information on 'political opinions', 'philosophical, religious convictions' or 'trade union membership' of the data subjects, as well as certain health data.

COMPANIES INVOLVED

Although the police files constitute an essential brick of the policy of maintaining order and surveillance in France, little information is currently available concerning the companies involved in the design of these databases or their storage. The same vagueness surrounding the software used by police, Gendarmes and intelligence services to process the data collected is essential for the surveillance apparatus of public authorities in France.

The processing of the TAJ file is done using tools developed in-house by the French law enforcement agencies, but also includes private partnerships. Since 2011,[79] the police have been using, first on an experimental basis, the facial recognition software "Facevacs Dbscan", marketed by the German company Cognitec, which works with many integrators such as Indemia and Atos.

[79] Gabriel Thierry (2019), l'Essor, "Why the legal challenge of facial recognition could make pschitt" https://lessor.org/a-la-une/pourquoi-contestation-judiciaire-reconnaissance-faciale-pourrait-faire-pschitt/

IMPACT ON SOCIAL MOVEMENTS

For the defenders of public freedoms, the multiplication of the various police files and their enlargement could have direct consequences on the activists. "The current law already allows the generalisation of the facial recognition of demonstrators," points out La Quadrature du Net. The TAJ, since 2012, technically allows facial recognition of demonstrators; to be registered, all you need to do is have been in contact with the police in connection with a court case.

The extension of the TASP, GIPASP and EASP files, for many observers, poses a real risk to individual freedoms since it allows citizens to be registered on the sole basis of their political idea, in particular in a context of the generalisation of drone surveillance. "If," points out La Quadrature du Net, *"via the global security law, all the demonstrators can be filmed in demonstration and that, via the TAJ80 file, a large part of them can be identified by facial recognition, the PASP and the GIPASP has already prepared a complete file for them in which to centralise all the information concerning them, without this surveillance being authorised or even controlled by a judge."*[81] A reform which according to them opens the door "to the massive filing of political activists, their entourage (in particular their minor children), their health or their activities on social networks."

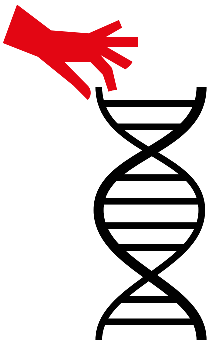
In August 2020, La Quadrature du Net, before the Council of State, attacked several provisions of the Code of Criminal Procedure authorising the police to use facial recognition to identify persons on the TAJ. On November 9, the association also filed an appeal with the Council of State against the extension of the Automated Control System (SCA) file. It similarly contests the extension of the TASP, GIPASP and EASP files.[82]

[80] Quadrature du Net website, "We are attacking facial recognition in the TAJ" https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/

[81] Quadrature du net website "Massive filing of political demonstrators" https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/

[82] Quadrature du Net website "PASP decrees: first battle lost against the massive registration of political activists" https://www.laquadrature.net/2021/01/07/decrets-pasp-premiere-bataille-perdue-contre-the-massive-filing-of-political-activists/

TREND 6:



INCREASING CENTRALISATION OF HEALTH DATA

An app to save them all, and in technology bind them together. Like dozens of countries around the world, France equipped itself, during the first months of the pandemic, with a contact tracing application intended to fight against COVID-19.

Announced in April 2020 and launched in June of the same year, the application, called Stop-Covid, then TousAntiCovid, struggles to take on; it has only gained interest from 14% of users and out of the entire population,[83] it has 1.6 million users (2.4% of the French population).[84] In January 2021, the government claimed to have nearly 12 million users. Figures that many media sources deem unreliable[85]

[83] Clément Pouré & Clément le Foll (2020), Médiapart, "'StopCovid', a French fiasco" https://www.mediapart.fr/journal/france/290920/stopcovid-un-fiasco-la-francaise?onglet=full

[84] Xavier Demagny (2021), France Inter, "After seven months of existence, TousAntiCovid still does not have its 15 million users" https://www.franceinter.fr/societe/apres-sept-mois-d-existence-tousanticovid-still-does-not-have-15-million-users

[85] Sylvain Rolland (2021), La Tribune, "How the government manipulates the figures of Tous Anti-Covid" https://www.latribune.fr/technos-medias/comment-le-gouvernement-manipule-les-chiffres-de-tous-anti-covid-863808.html#:~:text=Manipulation%20des%20chiffres&text=%5BTweet%20du%20Premier%20ministre%2C%20Jean,'est%20pas%20le%20cas.%5D

as the executive was communicating on the number of accounts created on the platform and not the actual daily number of users.

La Quadrature du Net, digital specialists, but also several parliamentarians, quickly expressed concern about the nature of the project and its technical implementation. "We are still talking about an application whose principle is to know who is where at all times," noted, for example, one of the French figures in cybersecurity, Baptiste Robert, in April. While the government insists on setting up a pseudonymity system, the *sine qua non,* for protecting the lives of patients and sensitive medical information collected by the app, Stop-Covid does not allow real anonymity. *"It's just completely impossible,"* explains Marin Drago, a lawyer at La Quadrature du Net, who points out that *"Stop-Covid is a surveillance application and citizens are followed in their movements."*

Another problem is the data storage model. In April, Google and Apple were working on an application programming interface based on a decentralised system for countries wishing to launch their contact tracing tool, which will ultimately be adopted in most countries of the world – the French government is moving towards a sovereign tool based on a centralized infrastructure – and has been criticized for being less secure than a decentralised model.

TousAntiCovid, in particular, makes it easier for experts to popularise other digital surveillance tools. *"The application encourages you to subject your body to constant surveillance"*, points out La Quadrature du Net, *"which will strengthen the social acceptability of other technologies, such as facial recognition or automated video surveillance, which are currently widely rejected."*[86] This risk is all the more worrying given that France now intends to reform the management of this health data.

Launched at the end of the parliamentary mission on AI by deputy Cédric Villani,[87] the Health Data Hub project aims to create a national health database, of certain strategic importance and classified as sensitive with regard to the GDPR.

This data already exists. It has exploded between the health services (each large hospital, for example, accumulates information on its patients) and multiple national databases (that of the national health insurance fund, one of the most important in the world, has accumulated nearly 100 terabytes of data). The project, which aims to centralise this information, as mentioned in the health law of July 24, 2019 which endorses the reform, *"to promote the use and increase the possibilities of exploiting data, both in clinical research and in terms of new uses, in particular those linked to the development of artificial intelligence methods,"* and there are worries from both players in the medical world and associations for the defence of public freedoms.

[86] Quadrature du Net website (2020), "Our arguments for rejecting StopCovid" https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/

[87] Cédric Villani (2018), "Giving meaning to artificial intelligence: for a national and European strategy" https://hal.inria.fr/hal-01967551/document

In November 2019, Jérôme Hourdeau took over as journalist in charge of public freedoms at Médiapart.[88] He reports the questions of the CNIL, which is worried about the technical architecture of the project and the possibilities of leaks but also about opening health data to a much wider use – until then, they could only be used within the framework of "the accomplishment of the missions of the services of the State, for purposes of research, study or education" ; the health law opens their use to any "reason of public interest".

"In addition to the CNIL, continues the journalist in a long paper devoted to the subject, the Health Data Hub project worries many observers for several reasons. First of all, there is the extremely liberal vision of the mission behind the Health Data Hub, which aims above all to promote innovation and start-ups at the risk of offering French data to GAFAM."

In April 21, 2020, a government decree also came in which exacerbated the situation: due to the health crisis, the government decided to accelerate the launch of the platform to be collected, "for the sole purpose of facilitating the use of health data for the needs of managing health emergencies and improving knowledge about the COVID-19 virus using a large amount of health data. The real sticking point was the hosting of this health data by the giant Microsoft.

COMPANIES INVOLVED

The Stop-Covid project is supported by a multitude of players[89] and is coordinated by National Institute for Research in Digital Sciences and Technologies (INRIA). The National Information Systems Security Agency (ANSSI) is responsible for cybersecurity issues. Several French institutions in the medical sector are also participating in the project.

Capgemini, one of the largest digital consultancies, ranked among the ten most powerful in the world, worked on the software architecture of the application. Atos, Thales and Sopra Steria have also been involved in the project to which they occasionally contribute.

The maintenance and hosting of the application are billed to the State by the company Outscale, a subsidiary of Dassault Systèmes. The awarding of the accommodation contract did not go through a public procurement procedure.

[88] Jérôme Hourdeau (2019), Médiapart, "Health Data Hub: the mega file that wants to make our health data profitable" https://www.mediapart.fr/journal/france/221119/health-data-hub-le-mega-fichier-qui-veut-rentabiliser-nos-donnees-de-sante?onglet=full

[89] Written question from the deputy of Philippe Latombe (2020) relating to the anonymity of the developers of the StopCovid project https://questions.assemblee-nationale.fr/q15/15-28687QE.htm

The anti-corruption association Anticor applied the national financial prosecutor in June 2020.

The leading French software publisher and the second largest European publisher, Dassault Systèmes is for the most part owned by the Marcel Dassault industrial group, known in particular for manufacturing fighter planes.

The Health Data Hub is a public interest grouping, but Microsoft was chosen to manage the hosting of the platform's data through its Azure cloud service. A contested decision because it calls into question the sovereignty of French data.

IMPACT ON SOCIAL MOVEMENTS AND OTHER ORGANISATIONS

TousAntiCovid and the Health Data Hub project are not seen as measures specifically targeting activists or demonstrations but potentially impact all citizens. One of the main concerns for public freedoms, denounced by several researchers in the press in the case of Stop-Covid,[90] is the hypothetical cross between this health data and other information.

In early June, around fifteen associations and personalities also applied seized the Council of State to try to prevent the deployment of the Health Data Hub. The procedure was bad, but the fight is starting to bear fruit: on November 19, as revealed by Jérôme Hourdeaux in an article for Mediapart, the Minister of Health, Olivier Véran, made a commitment to the CNIL to put an end to the hosting of health data by the American giant within two years.

[90] Antonio Casilli, Paul-Olivier Dehaye and Jean-Baptiste Soufron (2020), "Stop Covid is a disastrous project piloted by apprentice sorcerers" https://www.lemonde.fr/idees/article/2020/04/25/stopcovid-is-a-disastrous-pilot-project-by-sorcerer's-apprentice_6037721_3232.html

CONCLUSION

COVID-19, EXTENDING THE FIELD OF SURVEILLANCE

Like the wave of attacks that hit France in 2015, the COVID-19 epidemic has provided a new excuse for French law enforcement and institutions to deploy security technologies in the public space. As France watched in disbelief in early 2020, as Chinese police officers used drones to ask citizens to respect confinement, the same happened in France same a few months later. Drones have been used to monitor large cities, but also sea side and remote corners where the police cannot venture on foot or by vehicle.

Many companies have rushed into the health breach, adapting their technology to market cameras to detect the temperature of individuals, respect for social distancing or wearing a mask. Technologies that French institutions, like the Council of State with thermal cameras in the town of Lisses, were initially opposed. But the security sector companies ended up winning the standoff over one of the individual freedoms, which comes second to a government battered by more than a year of health crisis.

On March 11, 2021, a decree published in the official journal authorised carriers to use smart cameras to observe how the wearing of masks in buses, subways or trains was respected. The National Commission for Informatics and Liberty, which in May 2020 had interrupted a first experiment on the Paris metro because it presented the risk of generalising a feeling of surveillance among citizens, changed its mind, estimating in early March that their use would allow the RATP to *"produce statistical evaluations on compliance with the obligation to wear a mask"* and *"adapt their information and public awareness actions."*

A symptomatic turnaround. COVID-19 has provided a pretext for deploying intrusive technologies in the public space, the use of which is part of a broader security shift, all the more worrying as the French government intends to toughen the repression of demonstrations. The so-called 'global security' law, validated by the Senate, will reinforce, among other things, the ban on filming the police, the generalisation of video surveillance by drones or even body cameras.

An unprecedented loss for the individual freedoms of the French population, while the government continues to extend the state of health emergency, as it was able to extend the state of emergency after the attacks that struck the country, before including it in common law. Elected officials, both national and local, hope to improve their image, asserting themselves as defenders of their fellow citizens and using the security argument as an electoral argument.

Another fight looms for associations defending public freedoms: that of facial recognition that the government would like to deploy during a large-scale experiment, the 2024 Olympic Games, which will take place in Paris. It will be a point of no return, since it would lead, as was the case during the 2008 Olympics in Beijing or 2012 in London with video surveillance, to an unprecedented extension of this technology in the public space.

Images:

Cover page:
Jeanne Menjoulet_ Manifestation
contre la loi sécurité
globale_30/01/2020

Inside cover: Photomontage
El primer paso blog Flickr
+ Pxfuel.com

Page 6:
Photomontage.
Original images Pxfuel.com

Current page:
Jeanne Menjoulet_ Manifestation
contre la loi sécurité
globale_30/01/2020

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 plateform 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:

NOVACT

suds Internacionalisme Solidaritat Feminismes

With the support of:

Ajuntament de Barcelona

ICIP Institut Català Internacional per la Pau

OPEN SOCIETY FOUNDATIONS