# Doing Action-Research on Algorithmic Urban Policing: IA-Powered Surveillance, Elusive Democratic Oversight

Félix Tréguer

# Doing Action-Research on Algorithmic Urban Policing: IA-Powered Surveillance, Elusive Democratic Oversight

Félix Tréguer*

July 2021**

**Abstract**

In this discussion paper, I present an ongoing research-action initiative looking at "Safe City" programs fast spreading across France's urban areas: the Technopolice project. The programs we are documenting consist in research projects as well as on-the-ground experiments where companies from the defence sector or specialised in the operation of network infrastructures, but also global competitors like Huawei and Cisco, can crash-test their "Smart City" security solutions with the support of public authorities, often at the local level and usually without proper legal framework. Applications consist in Big-Data-powered statistics on crime and predictive policing, automatic analysis of video-streams from CCTV cameras (including facial recognition and detection of suspicious behaviours) or of online social networks – technologies for which there is usually a strong IA component. To shed light on these deployments and the public-private assemblages developing them, we have been using FOIA requests and new French laws on "algorithmic transparency". We have engaged in litigation and won a few cases, which in turn is accelerating a process of legalisation. This discussion paper covers the lessons learned as well as the hurdles that our initiative faces, the difficulty in enacting meaningful democratic oversight over these programs as well as on the law enforcement tactics they entrench.

*Félix Tréguer is associate researcher at the CNRS Center for Internet and Society and postdoctoral fellow at CERI-Sciences Po. His research blends political history and theory, law as well as media and technology studies to look at the political history of the Internet and computing, power practices like surveillance and censorship, the algorithmic governmentality of the public sphere, and more broadly the digital transformation of the state and of the security field. He is a founding member of La Quadrature du Net, an advocacy group dedicated to the defense of civil rights in relation to digital technologies.

**This draft discussion paper was presented at the EWISS 2021 conference, for a panel on "Artificial intelligence and the control of 'algocracy' in security issues."

In this draft discussion paper, I focus on an ongoing research-action endeavour on new technologies of urban policing, an empirical case that can contribute to shedding light on the nature and structure of "algocracy" in security-related contexts. Here, I use the word "algocracy" in an analogy with "technocracy," referring both to the *network of actors* promoting the adoption of automated decision-making or computer-assisted decision-making across bureaucracies, and the *power structures* formed by socio-technical and public-private assemblages formed around algorithms.

One cautionary remark: Because my research in what is at the moment a side project is at a very preliminary stage, what I present here are for the most part fieldwork notes with little and only implicit theorisation.

# Contents

# Introduction

The "algocracy" story I would like to share starts in Marseilles where I live, in late-November 2017.

At the time, in the European media, we were hearing about the local experiments around social scoring in China, as well as the dreadful use of videosurveillance across the country. We also read about the growing resort to predictive policing software and facial recognition tools used by U.S. law enforcement. But at that point, all of this still seemed a bit remote from the European continent.

Then one day, with friends from the digital rights group La Quadrature du Net (LQDN, where I act as a volunteer member), we received a message from a journalist of *Le Monde*, the leading newspaper in France. She was looking to get a comment on a joint press release issued by the city council of Marseilles and that of Engie Inéo, a branch of the large French utility multinational (formerly Suez) specialised in computing. They announced that Engie had won a contract for establishing a "Big Data Observatory for Public Tranquility".

The press release presented the project as key in bringing about the "Smart City." By reading it, we understood that the Observatory was meant for the cross-analysis of multiple databases that had hitherto been left apart, coming from various public bodies like the local police, hospitals or the local transportation utility. But detailed information on the project was still scarce, and of course it completely overlooked the fact that, in essence, that Observatory was an actual surveillance infrastructure.

It was all the more strange to hear about that grandiose scheme considering that Marseille is a very segregated city, where marginalised communities are already prone to various form of police abuse or negligence. In many poor neighbourhoods, police stations are decrepit and the basic material conditions for welcoming citizens and residents and respecting their rights are not even met.

## It all started with a FOIA request

In an attempt to learn more about the project, I filed a "Freedom of information" request to the city of Marseilles to obtain administrative documents related to the project. In France, the 1978 Freedom of Information Act ("*loi sur l'accès aux documents administratifs*") is reaped with exceptions, but I thought I would would give it a try.

In early-February 2018, I still had received no answer from the city council, so I appealed to the administrative agency in charge of handling "freedom of information" disputes between citizens and public administrations. However, a couple of days after that appeal was filed, I received a large envelope in the mail: The city had finally sent me some key documents related to

the public tender on the "Big Data Observatory". Among them was a 88-page document meant for bidding companies. It went over the goals of the projects, the range of data sources it would draw from, its role in learning from the past to anticipate future events. After reviewing that document, it was clear that the project was actually a prototype for a Big Data-powered recommendation tools for police managers, a sort of ambitious replicas of the software rolled out by U.S. vendors like PredPol, HunchLab or Palantir. The document looked overly ambitious, but it offered a unique look at the nitty-gritty of the project.

After studying these documents and further desk research, another thing became clear: The Big Data Observatory had been in the works for some years – at least since 2014. How come, then, it was only four years later that we realized was was going on?

Further research would lead us to the conclusion that, rather than an aberration, the case of Marseille was part of an hitherto unnoticed trend across the country. For some time now, many companies in France and beyond as well as public authorities across France had been convening meetings, trade fairs, engaged in research programs around "policing in the Smart City." Marketers had even come up a new term for this: the Safe City.

## Launching the Technopolice project

After uncovering half-a-dozen "Safe City projects" across France, and convinced that there were many more to dig up, we decided to turn our preliminary research and analysis into a participatory research-action campaign: the Technopolice project.

The goal was two-fold:

- First, we sought to document Safe City projects across France through FOIA requests and desk-research and then make our findings part of the public debate.
- Secondly, we hoped to empower people opposing these projects.

In September 2019, along with the French Human Rights League, our small group of half-a-dozen of LQDN employees and volunteers launched the project with a dedicated website offering:

- news analysis and "action guides" (technopolice.fr),
- a public forum (forum.technopolice.fr),
- a document database based on the Uwazi software (data.technopolice.fr)
- an instance of Etherpads for collaborative writing tools (carre.technopolice.fr),
- a SecureDrop leaking platform (technopolice.fr/leak).

Through these online tools, we sought to provide people interested in countering the new deployments at the local level while opening avenues for collaboration between local groups.

# 1. The Safe City's Technological Mix

So what are the key technologies and applications underlying current "Safe City" programs and their alleged objectives?

In this section, to give a sense of how AI is being applied to the field of urban policing, I briefly present a few projects, which can be subdivided in two broad categories: Big-Data powered statistics and recommendations (including "predictive policing" features) and computer-assisted vision (so called "smart videosurveillance").

## 1.1. Big-Data powered statistics, predictive policing

### The Big Data Observatory in Marseille

In Marseille, according to a key document related to the public tender that we obtained, The Big Data Observatory for Public Tranquility consists in a a vast integration platform based on "Big Data" and "machine learning" methods, capable of "analysing what happened (yesterday)," "assessing the current situation (today)," and "anticipating the future or likely situation (tomorrow)" (p. 12). It is also quite clear on the fact that "the approach is particularly exploratory and creative" (p. 42). Caroline Pozmentier, former deputy mayor in charge of security and project leader, has explained that "this big data will only work if we assimilate all the information from the police, justice, marine and fire services, transport, roads, weather, etc." (p. 42).

The platform is indeed meant to aggregate multiple structured and unstructured databases, in particular that of the General Security Delegation (DGSEC) of the city of Marseille, which lists all the police reports, fines, and many other geolocalised data collected by municipal security actors. It also aims to include data from public hospitals or from the city's external partners, and in particular the state, which holds most of the statistics relating to crime. An data-sharing agreement has been signed between the city of Marseille and the prefecture (representing the state) which gives the city access to national data on protest and public events held in Marseille, while offering the national police access to the Big Data Observatory.

Among the other sources of data that might feed the platform in the future are private partners such as telecom operators and their aggregated statistics on the location of the population. It is the company – in that case Engie Inéo – which will have the task of approaching these partners and conducting the legal work needed for accessing their data troves. The

documents also mentions the monitoring of conversations on social networks such as Twitter or Facebook, whether to "retrieve publications whose themes are relevant to the city's security," to "anticipate the threat" and assess the "risk of dangerous gatherings by analysing tweets," or to proceed with the "identification of actors" by spotting "who is talking, who is acting, who is interacting with whom" (the City later claimed that no personal data would be included in the system). Finally, crowdsourcing is also in order. According to the document, "each citizen" will be able to "provide information in real time (text, video, photo, speed of movement, stress level, etc.) via a smartphone application or connected objects" (p. 20).

**Building the Safe City in Nice**

In Nice, since 2018, the French defence contractor Thales has been spearheading a consortium of more than a dozen companies and public research centres to build a Safe City. The "experimentation convention" passed between the consortium and the City of Nice describes a even-more complex system.

According to a document first obtained via a whistleblower, the goal is to create the "Waze of public safety." The document opens up by stating that the "the world is becoming increasingly urbanised" and moves on to point to "increasingly important threats." Among these, "natural risks," which may be linked to climate change, and "man-made risks" (crime, terrorism, etc.) are placed on the same level: there is no question of questioning the economic, social and political causes of these phenomena, and even less of acting on them. What matters is to "assess each situation in order to anticipate incidents and crises," to identify "weak signals" in order to provide "planning assistance," to propose "predictions based on scenarios," all in the context of "real-time management" through the exploitation of the "maximum amount of existing data" within a "hypervision and command centre." To help "decision-makers," the Safe City platform aims at "collecting as much existing data as possible and looking for correlations and weak signals" (p. 23), "developing new analysis and correlation algorithms to better understand a situation and develop predictive capacities" (p. 24).

Like in Marseille, the monitoring of social networks and other "open data" is in order, particularly for the "short, poorly written texts" excerpted from Twitter, which will be mined by semantic analysis tools and feed into sophisticated crowd management recommendations, rumour analysis and "monitoring the actions of certain individuals or groups of people" (here, the consortium's specialist is a company called GEOLSemantics). According to the mayor of Nice, right-wing politician and former minister Christian Estrosi, the project will bring benefits beyond public safety, allowing for "an eco-context favorable to innovation by strengthening its collaborations with large industrial groups, SMEs and local start-ups, particularly related to the

French Tech network, as well as the world of research."

### Sûreté Globale's partnerships

Another similar tool is being used by various police forces across the country: it is called Map Revelation and is developed by Sûreté Globale, a company based in Angers. We came across it while working on another "Public Safety Observatory" of Montpellier.

Map Revelation has been used for some time by national police forces – e.g. to track illegal migration. But in recent years, Sûreté Globale has pushed for local implementations. Its tool is apparently used in other French cities like Lyon, Lille, Montauban, Villeurbanne, Angers, or Colombes.

According to Sûreté Globale's website, the software "'provides predictive, graphical and geographical analyses of semis of points " composed, depending on the clients, of "delinquency events, incidents" or other events and then "reveals important places and moments, and predicts occurrences'. According to an online source, "this interactive software, combined with a geographic information system, makes it possible to map facts precisely and to act accordingly. Equipped with a predictive system, police patrols are adjusted according to need and the community-policing strategy is improved."

## 1.2. "Smart videosurveillance"

### XXII, a fast-rising start-up

In a wealthy suburb located in the west of Paris, a local start-up is fast-becoming a leader in "smart videosurveillance."

Founded in 2015 by a young entrepreneur by the name of William Eldin, XXII now claims around 70 employees. On its website, the company says it is "specialised in software development via computer vision in Artificial Intelligence." "We support private and public companies in their transformation and increase their performance with innovative solutions." Its home-grown algorithms now equip the hardware of large multinational companies like those of Genetec. But XXII is still crash-testing its algorithms.

To that end, the start-up has concluded partnerships with cities in the Paris Region. Saint-Ouen, a city just outside of Paris north-eastern boroughs, was apparently the first to do so in 2020. In a newsletter, XXII announced that partnership along with the launch of its "XXII Core product," a suite of "algorithms for the Smart City which aims to make our cities safer, to relieve the work of the agents of the urban security centres and above all to protect you on a daily basis with a real-time analysis." A FOIA request later revealed that the partnership proved inconclusive. In May 2021, a city official wrote to one participant in the Technopolice project, saying that "contrary to what is indicated in the newsletter of company XXII, the City

of Saint-Ouen-sur-Seine tested the beta software only for a very short period of time. Due to software malfunctions, the experiment was effectively cut short and the City of Saint-Ouen-sur-Seine did not enter into a contract with the XXII company."

Apparently, this setback did not discourage XXII, which pledged to beta-test its "Smart City algorithms" in a hundred cities by the end of the year 2020. In Suresnes, a city neighbouring XXII's headquarters, another partnership was launched in February 2021. For XXII, the goal is to test its product – now rebranded "XXIISmartCity" – a product described in the agreement as being still at an "experimental" stage.

On its website, XXII describes the range of possibilities provided by its product:

> Draw a zone and define the maximum time for temporary parking. Only static vehicles beyond this limit will be detected. Define the stop line and the position of the traffic light. If a vehicle passes a red light, an alert is activated. Define a safety perimeter to detect anyone entering the area. Define an area to be monitored and set a maximum presence time. Suspicious occurrences will be reported.

The convention with the city of Suresnes indicates that the percentage of errors of the algorithms implemented will remain, "to the extend possible," below 10%. According to the mayor of Suresnes in the municipal council, this collaboration is warranted by the fact that, unlike countries like China, "the problem of our French companies is that they do not have access to sufficient databases, image databases, event databases that allow them to also quickly train their algorithms." The General Regulation on Data Protection is implcity framed as a competitive disadvantage for French and European companies in the field, and some mayors are willing to help them out.

### Other automated videosurveillance projects

Many other French cities have implemented automatic video-analytic features to their videosurveillance systems. And sometimes, the technology provider chosen by local authorities contradict and oft-repeated mantra in elite discourse on digital policy: that of "digital sovereignty." In Toulouse for instance, the city police is working with IBM. In Valenciennes, Huawei has provided the city police with 230 cameras equipped with video-analytics software, free of charge. Next to Grenoble, in the small village of Moirans, the city launched a public tender to buy a few videosurveillance cameras, and chose a bidder which offered to come up with next-generation, AI-powered tools – in this case, the company supplying the software through a French subcontractor is the Israeli firm Briefcam. Briefcam's tools have also been used in Lille or Vannes.

Marseille too has been looking to experiment "smart videosurveillance" until La Quadrature du Net introduced a legal challenge. One of the documents we obtained regarding that experimentation alleges that "operators cannot visualise all the flows" and that "it is therefore necessary that the software solution allows for this visualisation to be carried out autonomously." How so? The software will offer "automatic processing of data (...) in order to detect anomalies/incidents/remarkable events" drawn from the video footage and will allow for the "detection of anomalies not identifiable by an operator," facilitating the "management of public space" through the "analysis of pedestrians/vehicles as well as behaviour."

There too, we find the typical use-case for these systems: automatic detection of "abandoned objects," of graffiti, of "theft, disappearance or destruction of street furniture." The technology should also assist in criminal investigations, allowing for "searches using filters" in the videosurveillance archives (stored one month), with one of these filters allowing for the identification of "individual (description, avatar, photo)" and the automatic retrieval of video footage where she or he appears. A final section entitled "Provision and integration of additional functionalities" makes clear that the city might later ask for additional features like "sound detection" (explosion, gunshot, etc.), "event reconstruction" (such as the route taken by an individual) or the detection of "abnormal behaviour" (fight, raiding, assault).

## Algorithmic transparency?

In concluding this section, I would like to make a few observations about our inability to describe in greater detail the technology at hand: In several instances, we have been using a legislative provision adopted in 2016 and creating a new transparency obligation for "algorithms" used by public administrations. So far, the results have been rather uninteresting.

In one instance, the city of Marseilles gave overall information about the "Big Data Observatory,"[1] but in other instances, local authorities invoked trade secrets to refuse disclosing documents. In Moirans, the FOIA agency

[1]Here is what the director for legal affairs of the City of Marseille wrote us : « "We are also providing you with a document answering your questions about the algorithms used in the project [note: no document received on this point - I have followed up with the DAJ], which will also confirm for the third time that no personal data is collected. In detail, the following data are used as factorial axes to identify similar events in the past: Location / Number of participants / Nature / Sector / Is during the week / Is during the weekend / Is in winter / Is in summer / Right of way / Duration. The algorithm used for the learning model is based on decision trees. These trees are constructed by the "random forest" algorithm. From the moment when similar past events are interpolated, the facts found around these past events are "transferred" to the predicted event or more precisely the score elaborated for each past event from the combination of the facts found is transferred to the predicted fact." (source).

ruled that we should have been granted access to the user manual of the Briefcam software (which EFF has already published in the U.S.).

More systematic attempts at shedding light on the nature of the algorithms used in the context of urban policing are underway. But thus far, FOIA requests usually do not return interesting information about the name of the product used, the identity of the contractor, the source code, or even impact assessment reports. And for the most part, it seems that public administrations are reluctant to apply the law in its full scope, and cherry-pick the documents that they send U.S. (we're considering strategic litigation on that front). When enough information can be found through other means, another possibility to find more detailed descriptions of Safe City technologies would be to look at research papers and patent filings.

Also, due to structural opacity, looking at the actual practices has thus far remained a challenge. Our team mixing researchers, activists and technologists is not being granted access to CCTV centres and other command centres where these technologies are being integrated in security practices. Because most of these projects are still quite experimental, and because these technologies are fairly recent, our FOIA requests return very little information on the status, relevance, assessment of on-the-ground use. Other sociologists working on Safe City programs in France have also reported having a hard time having access to interviewees. Opacity remains the rule, and one has to come up with ad hoc research tactics to pierce through it.

## 2. Public-Private Hybridisation

After this overview of the technologies used in Safe City programs across France, I now turn to the public-private assemblages working to foster the use of Big Data and AI-based algorithms across the security field.

Several socio-technical and political trends play a role in the advent of the Safe City in France – for instance, the rise of securitarian governmentality and of the "Penal State", technological solutionism, the quest of rationalisation and optimisation in bureaucratic organisations, the race to data governance across public and private bureaucracies. But one of the most striking of these factors is the extent to which the rise of Big Data and AI-powered policing technologies appears to be overdetermined by, firstly, the perception that global power will depend on mastering these technologies, secondly, the formation of huge markets for which there is a perceived need to ensure that home-grown companies will be able to seize their shares in the face of Chinese, U.S. or Israeli competitors. Indeed, Safe City projects are at the crossroads of two very promising markets. In 2020, the "Smart City" market was estimated at 410 billion dollars. Market studies predict 15% growth between 2019 and 2025, which will represent more than 675 billion dollars worldwide by 2028. And the security market, all sectors combined,

represented 629 billion euros in 2018, increasing by 7% per year, i.e. twice the global growth rate according to numbers released a few months before the Covid-19 pandemic.

These various factors have led to the flourishing of social networks of "algocrats" promoting the Safe City across the policy spectrum. These networks combine various intertwined categories of actors:

- public officials from the security field (police, intelligence, military) but also civil servants working in research and industrial policies;
- security entrepreneurs often coming from the private sector – whether from start-ups or multinationals – sometimes also with a foot in academia (e.g. teaching business classes, criminology, or data science);
- local and national politicians working to shape public opinion and public policies in a way that will legitimise and speed-up the roll-out of Safe City projects.

## 2.1. Cross-socialisation

The coming together of public and private actors unfolds in many complex ways. Cross-socialisation in elite schools and frequent circulation between public administrations and large corporate firms ("revolving door") seem to be a common feature of these public-private assemblages promoting forms of algorithmic automation in security practices. Two examples that can help give a sense of these social trajectories:

- Thales; the French multinational and leading defence contractor (where the French state is a significant shareholders with about a third of voting rights on the company's board), is currently headed by Patrick Caine (born in 1970), who became CEO in 2014. After having graduated from two elites schools – Polytechnique and Mines –, Caine worked in the private sector and then worked for the prefect of the Franche-Comté region. From July 2000 to February 2002, the thirty-year-old joined the Jospin government as a technical adviser in charge of energy to the Secretary of State for Industry, Christian Pierret. In 2002, he moved on to work at Thales' Directorate for Strategy and quickly moved up the ladder.
- Cédric O (born in 1982) is Deputy Minister for Digital Affairs and one of the leading proponents of facial recognition in France. He is a graduate from France's top business school HEC Paris (2006). Freshly out of school, he worked in the private sector while working a political adviser (of Dominique Strauss Kahn in 2006, of François Hollande's campaign in 2012, before joining Macron's bid for the presidency in

2016). Between 2014 and 2017, he worked at Safran as a project manager for the group's industrial director and then as production manager at Safran Aircraft Engines, part of the Safran group, a leading technology company and defence contractor. In 2016, Safran sold its biometrics division (Morpho) to another French biometric company called Oberthur Technologies, leading to the creation of Idemia (also with a minority stake of the French government and about a third of voting rights).

The 2017 leak of the Macron presidential campaign also offers a glimpse of the forms of cross-socialisations between algocrats. In one of the email threads from December 2016, the team in charge of advising Macron on security affairs discusses the opportunity to establishes a digital identity card ripe with biometrics. Among the participants to this rather informal group, we find François Heisbourg, a geopolitical expert and former director of Thomson CSF (the company that would later become Thales), but also Marianne Tarpin, a senior official of the Directorate General of Internal Security (DGSI, the main domestic intelligence agency), and Anne Bouverot, then CEO of Safran's Morpho (now Idemia), the French leader in biometric identity.

Of course, private sector lobbyists work actively to nurture these public-private relationships. AN2V is the main French lobby for videosurveillance vendors active in France. In January 2019, the organisation held its "night of AN2V" reception. Among the guest speakers that night were Jean-Michel Fauvergue – a former head of the National Police's elite tactical unit who retired in 2017 to join Macron's party and was elected member of Parliament – and Luc Ferry, a philosopher and former Minister of Education and Research in a right-wing government.

## 2.2. Formal cooperation

Avenues for cooperation between public and private sector elites can of course be more formal.

When the computer vision start-up XXII set up an "ethical committee" last year, it reached out to Renaud Vedel, a prefect that has been in charged on AI at the Ministry of the Interior, and Emmanuel Goffi, a former military officer turned professor at Institut Libre d'Étude des Relations Internationales (ILERI) in Paris, and a member of GICAT.

In other cases, civil servants representing the state and private executives sit on the same corporate boards. I have already mentioned the French government's stakes in Thales and Idemia. But representatives of all three entities also sit together on the board of a company called Civipol. Presented as the "technical cooperation operator of the French Ministry of the Interior, " the French state holds a 40% share in this entity designed to

export France's security and policing know-how and technologies abroad, so as to help position French corporations in foreign markets.

Over the past decade, several organisations designed as an interface between France's security industry and the government have been created, such as the CoFIS (*Comité de la Filière Industrielle de Sécurité*). Established in 2013, COFIS's goals is to promote the interest of security industries at the government level. Or, as the CoFIS puts it on its website (actually a subdirectory of the French government's website), "the ambitions of the committee of the industrial security sector are to develop the necessary means to face the threats and risks likely to affect the life of the Nation and to support the activity of the French security industries through a renewed public-private dialogue." CoFIS's personnel mixes business leaders and high-ranking civil servants working on national security, who sometime also sit in other similar structures, like the CICS (C*onseil des industries de confiance et de sécurité*), which act as a larger umbrella for the security, defence and aero-spatial sectors.

But how does CoFIS – whose name changed in November 2018 to *"Comité stratégique de filière pour les Industries de Sécurité"* after it was formerly recognised as part of the National Council of Industry, and now headed by Marc Darmon, Deputy CEO at Thales – work towards achieving a "renewed public-private dialogue" exactly, and what power does it have in advancing Safe City projects? CoFIS's website gives a few hints. It explains that CoFIS will "draw up an overview of security needs through a renewed dialogue between the State, public and private operators, research centres and industry." It also frames its role as that of developing, "at the best cost, innovative security solutions, adapted to the real needs of national users and globally competitive, in collaboration with all the players: prescribers, users, research centres and industry." Thirdly, CoFIS' role is to launch:

> projects that meet priority needs and make it possible to strengthen the competitiveness of the French offer on the international scene. These demonstrators will be either advanced product prototypes or integration, test and demonstration platforms.

For the most part, these prototypes and demonstrators are the kind of projects that we document through the Technopolice campaign.

In January 2020, the ministry of the Interior, the ministry of Industry and CoFIS signed a "strategic contract" listing the various priorities for the years 2021-2022. Among the key "axis" listed in document, we find the need to "develop a global offer to secure major events with a view to the 2024 Olympic and Paralympic Games," but also biometric "digital identity" and "Trusted Territories" – another word to refer to Safe City projects –, so as to "ensure ethical French leadership in the security of the smart and connected city, through global solutions for local authorities."

On this third topic, the goal is to "bring out the needs and uses supporting the transformation of intelligent and secure territories." To that end, companies are committed to developing "ethical guidelines" for the implementation of these systems, but also to start a working group including private actors and local authorities, and finally to document the various actions conducted over the period.

As for the government, its committent lies in "raising the awareness of local authorities regarding the importance of security and sovereignty of intelligent territories," "contributing to the analysis of the needs via the mobilisation of public players" while working with local authorities to "communicate on the action and the issues at stake, in a national and European framework." Later in the document, while industry players – and in particular AN2V will have to deliver a "report with reasoned proposals for legal and regulatory changes" in 2021, the government commits to "support the proposed legislative and regulatory developments." Basically, the government acknowledges that it will let industry players draft the law regulating this controversial surveillance technologies.

Similar inter-meshing of private and public interest also takes place at the European level. Groups like EOS, the "European Organisation for Security" – which frames itself as "the voice of the European security industry and research community" – includes companies like Thales and Idemia. Funded by a former Thales executives, Luigi Rebuffi, it acts a think-tank making recommendations on research policy. For this purpose, EOS sets up working groups. For instance, EOS' working group on "border security" says it "engages directly with the European Commission, European Parliament, European Council, and EU Agencies (Frontex, eu-LISA)." Rebuffi has also been a member of the Protection and Security Advisory Group, which:

> ... provide[s] consistent and consolidated advice to the Commission Services during the preparation of the Horizon 2020 Work Programme, regarding the Secure Societies Challenge of the Specific Programme.

## 3. Surveillance Across the Policy Spectrum

We could go on an on to retrace these complex public-private connections. In offering a few examples to illustrate the point, I cannot account for the struggles and logics of distinctions that occur within the algocrats' social space (in-depth field interviews would be necessary). But these various examples help understand how "Safe City" programs come to permeate a wide range of policies and administrative levels.

### 3.1. Research policy

A key locus of the policy process driving Safe City programs lies in research policy. For instance, we know that groups like EOS have played an important role in shaping new research programme "Horizon Europe," which now has an entire cluster dedicated to "civil security for society," with all research dedicated to fundamental rights being now in another cluster called "Culture, Creativity & Inclusive Society"). EU research is key considering that the European Union's commitment to the research and development (R&D) of surveillance technology has risen steadily over the past years in the context of the Horizon 2020 research program, which represented 50% of the overall public funding for security research in the EU, according to a EU Commission report. In France, CoFIS also boasts about the fact that, thanks to its action programme, "the security and cybersecurity of infrastructures have been identified [...] among the priority actions of the national research strategy."

To give an example of how private influence materialises, consider this call issued in March 2019 by the European Commission's research division on "smart and safe cities", which recycled some of the language it has been used over and over in such calls over the past decade:

> The security and good operation of a smart and safe city relies on interconnected, complex and interdependent networks and systems: public transportation networks, energy, communication, transactional infrastructure, civil security and law enforcement agencies, road traffic, public interest networks and services offered by public and private operators. Such networks provide with an efficient infrastructure for detection resources and 'big data' collection. The screening of such data are being used by security practitioners to enhance their capabilities and performances.

Overall, EU funding of security-related technologies more than doubled over the past years, from about 3.8 billion euros for the 2007-2013 budget cycle to 8 billion euros for 2014-2020, a Statewatch study found. As for the 2021-2027 Horizon Europe programme, budget discussions secured a 30% increase for overall research and innovation programmes. Over the past decade, a company like Thales has received hundreds of millions of euros in public funding through European research grants.

### 3.2. On-the-ground experiments

Downstream, once the basic R&D is finalised, a key phase lies in "bringing out the needs and uses supporting" the Safe City, that is to convince

local authorities and the population at large that these surveillance technologies are efficient and "acceptable." To that end, they of course receive support from local authorities. These partnerships – and the kind of projects I discussed in the first section – are often presented as a win-win: companies offers the technology for free or at reduced cost, and in return it benefits from a full-scale test of its technologies while starting to bind civil servants to its products.

In Suresnes, the agreement concluded between XXII and the city provides for four things. First, the presence, without time limit, of an operator of XXII within the premises of the city's CCTV centre. Second, the city's commitment to provide all necessary information for the project. Third, the existence of a technical committee partly composed of members of the CSU, which should meet "as often as necessary to promote the smooth running of the project." XXII will thus benefit from the active collaboration of public officials, transformed for the exercise into beta-testers responsible for identifying the bugs and errors present in XXII's products. Fourthly, XXII will also be able to use the Suresnes CSU as a real laboratory at the service of its technical teams. This provision of public resources for the benefit of XXII will greatly facilitate one of the main hurdles faced by companies developing automated video surveillance algorithms: The labeling of their databases.

The contract also makes clear in several excerpts that XXII will own the databases used and created through the experiment. It is specifically written that XXII is co-owner of the "results" of the experiment, the latter being defined in particular as the "knowledge, variables, [...] database" obtained during the term of the agreement. Finally, just like in Nice, the agreement provides that XXII will be able to use the Suresnes CCTV centre as a showroom for potential clients.

But public funding does not stop there. In Nice, the Safe City started by Thales benefited from 11 million euros in the form of grants and recoverable advances from France's public investment bank (BpiFrance), for a total project cost of 25 million euros over a three-year period. France's National Agency for Urban Renovation (ANRU) has also provided funds for some of these projects. That is the case in Saint-Étienne, where the mayor worked hand-in-hand with a start-up owned by the local group Verney-Carron (a leading supplier of rifles for the French army).

In Saint-Étienne, the goal was to install microphones in a marginalised neighbourhood of the city centre to detect, through algorithms trained on Machine Learning, suspicious sounds. Eventually, the idea was to automatically send drones to the scene and provide video to conduct so-called "removal of doubt" operations. This experiment was stopped by the French data protection authority, the CNIL, after we obtained FOIA documents on the project and after local activist groups started making some noise. In Marseille, the Big Data Observatory has been funded with a 600 000 euros grant coming from European FEDER funds.

### 3.3. Long-term planning

In November 2020, the French government issues its long-term plan for the Ministry of the Interior by publishing a *White Paper* on Internal Security. Renaud Vedel, the prefect in charge of AI at the Ministry and member of XXII's ethical committee, led the process leading up to this release.

This planning document makes no less than two hundred recommendations to beef up security policies. In the name of "recreating the conditions for trust between the population and the security forces", the White Paper hints at a massive effort to strengthen the Interior Ministry's public relations strategy and to create avenues for citizen participation in policing duties. To ensure "coherence between all actors in the security continuum", it envisions extending the power of the ministry over municipal police forces and granting evermore powers to private security firms. To provide for "the human, material, and technological resources" needed to meet its ambitious goals, the document submits that 1% of the French GDP should be invested in security policies by 2030, which would result in a 30% budget increase over the next decade.

Part of those sums are meant "to take the Ministry of the Interior to the technological frontier". Here, the White Paper gives a good overview of all the surveillance technologies currently making their way out of the industry's R&D labs. It calls to experiment with biometric identification not only through facial recognition but also the analysis of voice and body odors, as well as using AI "to deal with the growing volume of information." It foresees multiple command-and-control centres fed with Big Data to provide for "the analysis of past data as a tool for retro-control and decision support," or asks for vastly expanding the use of surveillance drones.

The recently-adopted *Bill on Global Security* lays the groundwork for much of the White Paper's content and represents the first building block of the long-term plan put forward in the document. Though the Bill's provisions were heavily struck down during a *ex ante* review by the Constitutional Council – in particular the provisions legalising police drones, the government has vowed to present a legislative patch in the coming months.

## 4. Weak Oversight

As part of this Technopolice project, we have mobilised the law before the courts, which has led to a few small victories. For example, we obtained a ruling prohibiting the use of biometric systems such as facial recognition to manage the entrances and exits of high schools in Region Sud (which includes Marseille and Nice). This ruling was not a given: Consulted over the plan, the CNIL had first seemed to think that this type of application would be acceptable under certain conditions. As mentioned before, the experimentation of "intelligent microphones" in Saint Étienne was also blocked

by the CNIL. We also have a case pending before the Marseille Administrative Court against automated video surveillance, which we hope will set a precedent across the country.

But these are temporary victories. The law can be a tool but it cannot account for all the issues raised by these techno-police deployments. Many of the legal safeguards that have been put in place over the past forty years to curb the most problematic aspects of computer technologies are proving ineffective in practice to stem the tide of surveillance systems.

The CNIL is a rather paradigmatic institution in this respect. It was created in 1978 following the first major controversies surrounding computer surveillance and state filing, and even though it has sometimes tried to resist and slow down the development of surveillance, it remains structurally locked in a form of impotence. Very often, it sees itself as an institution responsible for accompanying technological progress. It will therefore retreat into calling for the adoption of safeguards to control the use of such and such technologies, but will prove incapable of enforcing them in practice. And if it ever does – which remains quite exceptional – the government will either ignore its opinion or use the next security crisis to change the law and overcome its opposition.

In fact, the CNIL's prerogatives have been declining for almost twenty years. In the 1990s, for example, it was quite vocal in opposing the deployment of video surveillance and the creation of large police databases, and in 2004 a reform removed its power to block the government's creation of new surveillance programmes – its opinion became merely advisory. The European General Data Protection Regulation (GDPR), which came into force in May 2018 at EU level, also removed some of its powers, including the power to authorise – and therefore block – surveillance schemes at local level.

Hence, even if the CNIL acted in a few instance on which citizen and media attention had built up, it remains unable or unwilling to keep track of all the controversial projects making their ways across French cities, and much less act to remedy these initiatives which are in most cases in breach of European privacy rules. There appears to be similar oversight gaps all along the process driving the spread of new policing technologies, including in the context of EU research programs.

In short, counter-powers exist but appear relatively weak compared to the strategies of the algocrats, who are well positioned throughout the field of power. And for several months now, partly in reaction to citizens' mobilisations, we have been witnessing processes of legalisation of Safe City projects.

## Conclusion: Towards the legalisation of the Safe City

French algocrats promoting "Safe City" technologies have a plan: To take advantage of the Paris 2024 Olympic Games. Emulating the experience of Beijing 2008, London 2012, and Sotchi 2014, they want to turn the event into a real-world demo of the French know-how in techno-policing, securing business opportunities and ensuring the 'social acceptability' of these controversial technologies in France and beyond.

In October 2019, the Minister for Digital Affairs Cédric O paved the way for this plan when he declared that "experimenting with facial recognition is necessary for our industry players to make progress," striking a techno-nationalist vibe keen on promoting the interests of French industry players. But thus far, in order to avoid public backlash, Macron's government's preferred strategy has been one of "small steps" – authorising what Cédric O called "limited, controlled and supervised use" that would seem benign enough but would help normalise the public to these technologies. Indeed, this is precisely what the government did in February 2021 when it adopted an executive decree authorising RATP – the public transportation operator in Paris – to plug its CCTV network to the video-analytics technologies of a start-up called Datakalab, in order to gather statistics on the number of people wearing masks during their commutes.

The problem for Mr. O and other promoters of automated videosurveillance is that this low-key legalisation strategy not only bypasses Parliament but also violates several principles enshrined in European privacy rules, and in particular the General Regulation on Data Protection. Hence, if the French surveillance industry is to be ready by 2024, a new legislative framework is urgently needed to secure and expand the rolling-out of new surveillance technologies. Didier Baichère, a member of the majority in Parliament, has set out to do just that by preparing a dedicated legislative proposal focused on the experimentation of facial recognition and the use of AI-powered videosurveillance.

At the European level too, the recently-tabled proposal for a "Artificial Intelligence Act" might actually carve out exceptions tailored for "public safety" that will take precedence of the GDPR and the police-justice directive to legalise many applications of automated videosurveillance. Predictive policing technologies, which were considered "high risk" and subject to more protective safeguards (conformity assessment, human oversight, etc.) in a previous version of the draft legislation, were later taken out of that category. That being said, there might be a chance to emulate the work of activist groups and city councils in the U.S. to enforce a blanket ban on various forms of Big-Data surveillance.