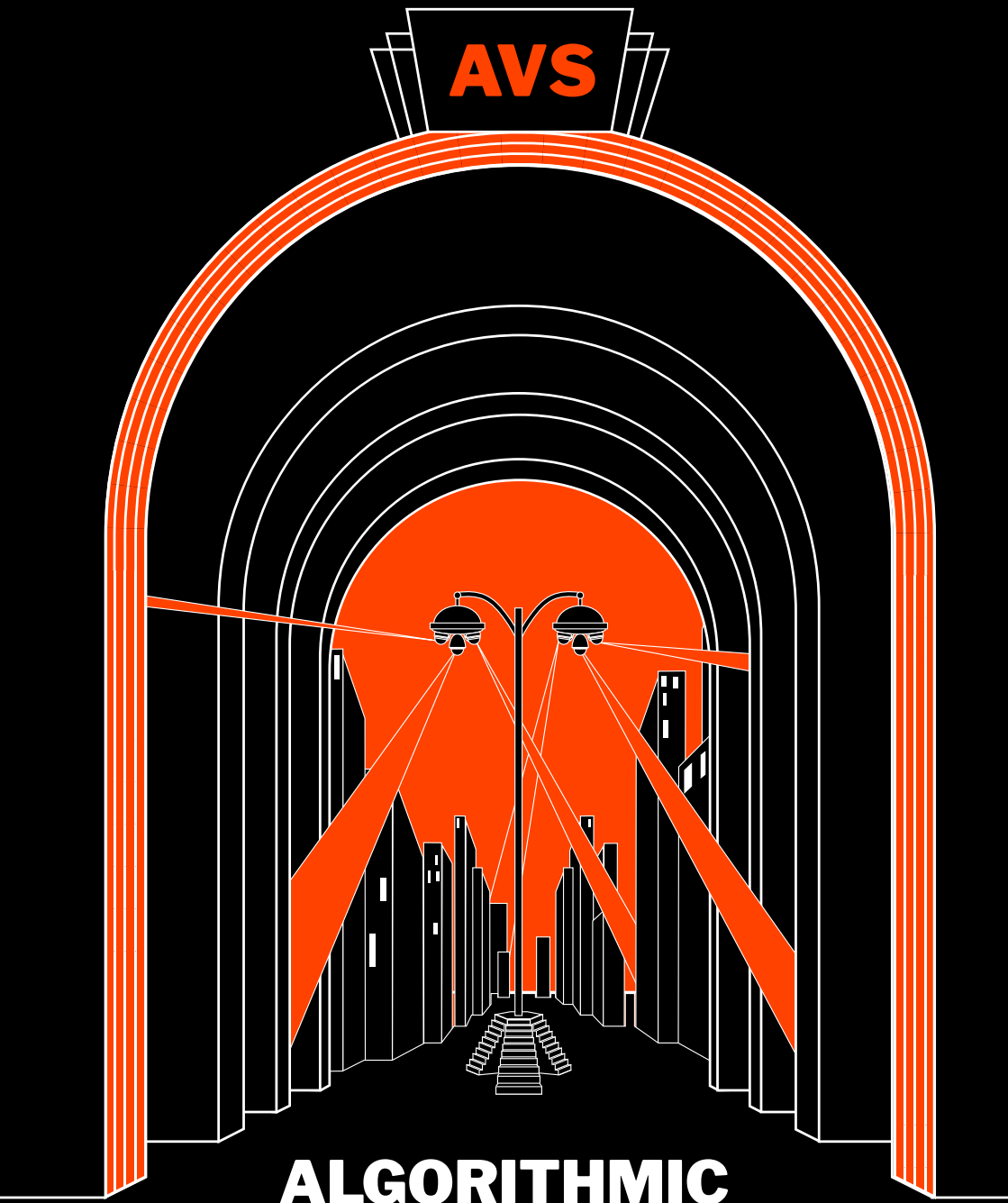
AVS



ALGORITHMIC
VIDEO SURVEILLANCE
DANGERS AND COUNTER-ATTACKS

Automated analysis algorithms for video surveillance systems are everywhere in our everyday lives, whether we realize it or not. Algorithmic video surveillance, or AVS, can have a significant impact on our liberties, often without our knowledge or consent.

These security algorithms are typically designed to be as invisible as possible. Their creators go to great lengths to integrate them into urban furniture, conceal their automation mechanisms, and make them as unobtrusive as possible. The goal is to normalize their presence and the effects they have on social control.

AVS technology is a new tool for law enforcement. It adds a software layer to the cameras that are already present in cities, allowing for the analysis, classification, and categorization of our bodies and movements. This fits in with the broader vision of the 'Smart City," where video sensors and algorithms work together to turn everything into data, make predictions, and identify 'weak signals."

Video surveillance has been spreading rapidly in cities across France, often illegally slipping in under the radar. Those who advocate for 'technopolicing"—a group that includes ministers, top officials, surveillance industry executives, machine vision engineers, and more—have been spinning a new narrative, rebranding the algorithms that drive these camera systems as 'smart" and 'augmented." These systems are now marketed as 'video protection," and the algorithms are said to 'optimize" and 'rationalize" police actions.

But in reality, they are part of a larger ideology that promotes total surveillance and systemic repression.

As these 'legal" video surveillance experiments are now being rolled out nationwide in France, thanks to laws related to the 2024 Paris Olympics, it is important to understand the political and technical implications of the algorithmic surveillance of our bodies through video monitoring.

This report, based on years of activism, investigations, analysis, and legal challenges by La Quadrature du Net and local Technopolice collectives, aims to demystify the algorithms that power video surveillance systems and their historical, political, and economic context. By understanding these technologies, we can better detect, circumvent, and denounce them, and imagine a brighter, liberated future for our cities and communities, free from the pervasive surveillance inherent to the 'smart city" and the oppressive tendencies of technopolicing.

Table of contents

Introduction:
What is Algorithmic Video Surveillance (AVS)

Algorithmic Video Surveillance (AVS) refers to software used by the police that analyzes images from video surveillance cameras. This software is designed to detect, identify, or classify specific behaviors, situations, objects, or people. These types of software are created by private companies and are based on computer vision algorithms, a technology that uses statistical learning to isolate specific information from static or moving images. Through machine learning techniques (one of the methods associated with “artificial intelligence”), algorithms are trained to automatically detect certain elements.

These programs are primarily used by the police in connection with video surveillance cameras: either for real-time detection of certain “events” or in delayed mode as part of police investigations.

Real-time alerts allow a smaller team to detect “events” of interest to the police from a large quantity of video feeds. The software automatically detects situations perceived as suspicious or risky and alerts the agents present in the Urban Surveillance Center (USC), the equipment room where video feeds are routed for viewing. In practice, AVS aims to detect objects (such as a suitcase or garbage bag), features related to people (somebody lying down, graffiti artists, clothes), or events (such as somebody crossing a line, people gathering…).

While it is trivial to search for something in a text document, the task is more complicated and time-consuming when it comes to searching in a video feed. AVS can be used after the fact in investigations to automate searches in video archives. It consists of launching image recognition queries to retrieve all the video data related to certain thematic criteria. For example, detecting all men wearing a yellow t-shirt and black pants in a given geographical area over the past 24 hours. AVS can also shorten the viewing time by condensing hours or days of videos into a few minutes. The role of AVS in this case is to select the moments likely to be of interest to the police and to skip the rest of the video.

It should be noted that these two uses of AVS (in real time and after the fact) are based on the same automated analysis process and therefore do not need to be distinguished from a technical point of view.

This analysis work was previously done by people, mainly city agents, or municipal police in a USC in the case of public video surveillance cameras.

AVS is Destroying Our Cities and Our Lives

Algorithmic video surveillance (AVS) is fundamentally changing how we interact with our urban environment, in ways that are consistent with a long-standing political view of public spaces as sites to be secured and controlled. In practice, AVS strengthens social norms that marginalize the most vulnerable members of our society and gives law enforcement new and significant powers of repression.

A AVS: The Fantasy of Security

The fact that behavior detection algorithms can now be a part of the surveillance arsenal is due in no small part to a security-oriented vision of the city and society, which has been present in the political landscape for several decades.

"Public disorder" as an ideological driver

The primary rationale for deploying AVS is the same one used to justify the installation of surveillance cameras in public spaces: to combat "public disorder." However, this term is not based on any concrete facts or precise measurements of crime, but is instead a political construct produced by public authorities since the 1970s.

In reality, public disorder is a subjective feeling that varies based on sociological factors, perceptions, and experiences. As researchers Philippe Robert and Renée Zauberman have argued, "public disorder" is a concept that combines two distinct ideas: first, a concrete fear of harm to oneself or loved ones, and second, a more abstract concern about how to address delinquency as a societal issue.1 Public disorder is therefore rooted in personal experiences and perceptions, rather than objective reality.

1 Philippe Robert and Renée Zauberman, *Du sentiment d'insécurité à l'État sécuritaire, Le Bord de l'eau, 2017.*

It was first taken up as a political issue in France after the end of the "Glorious Thirty" (1945–1975), a period marked by the rise of job insecurity and mass unemployment. From that point on, the political treatment of crime shifted from a focus on identifying individual offenders to managing crime as a mass risk. The way that citizens experience crime (and not just its victims) became central to this new approach, leading to a proliferation of laws, declarations, and announcements.

Over time, leaders have used this fear of disorder to promote an authoritarian vision of security in public spaces. This fear is constantly stoked through sensationalist news stories, the visible deployment of repressive measures, and surveys measuring "public order concerns."

Deployment of Security-Oriented Urban Planning and Video Surveillance

In the 1980s, public security policies integrated prevention, social policies and local components. Today, however, these policies are largely driven by the Ministry of the Interior and focus on repression, with crime prevention through environmental design as a key strategy. This approach is based on the idea that crime can be prevented or reduced by modifying the environment in which it typically occurs. In practice, this means changing the layout of public spaces to discourage criminal behavior. This involves, for example, making streets less dark or reducing the number of nooks and crannies.2

Crime prevention through environmental design has been one of the driving forces behind the deployment of video surveillance, in a context marked by the decline of social action. **It feeds the distorted view that disorder is mainly to be found in public spaces**

2 For further information on crime prevention through environmental design, see Circulez , la ville sous surveillance by Thomas Jusquiame, Ed. Marchialy.

by playing on the fears described above. Cameras have gradually replaced social workers in the streets. As a result, **all other forms of insecurity**, whether **social** (housing insecurity, unemployment), **societal** (pollution, sexism, racism) or **health-related** (malnutrition, addictions) **are neglected**.

Through video surveillance and its algorithmic counterpart, "street incivilities" and their repressive treatment are highlighted, overshadowing other illegal acts and alternative approaches to violent or deviant behavior. Under the pretext of improving security, **it is an attempt to discipline the lower classes. In fact, the primary victims of AVS are the people living on the streets.** If their safety had been a genuine concern, then one of the priorities would have been to provide housing for the more than 600 homeless people who died on the streets in 2022 in France. And while the police scrutinize the streets and over-criminalize populations subject to structural discrimination, white-collar criminals are getting less and less attention.

Women's safety is a prime example of this situation
According to this repressive point of view, the danger of violence and rape is said to be primarily located in the (preferably dark) street and the solution would be to install surveillance cameras to protect and *reassure* women.

However, available studies and figures are clear: women are most in danger at home, at work, or in other private spaces. In 91% of cases, attacks are committed by someone known to the victim (their partner or ex-partner in 47% of cases). And recent observations show that the political response should not be solely repressive, but rather a deep transformation of society through institutional changes, prevention, support, and training. As for safety in public spaces, a priority should be to change behaviors, given that more than 88% of witnesses do not react to incidents and sexual assaults and that, whether cameras are there or not, the police will be largely ineffective in taking and processing a complaint for sexist or sexual violence.

Source : Source: The Conversation, "La sécurité des femmes : une question surtout domestique," November 24th, 2021, at https://theconversation.com/la-securite-des-femmes-une-question surtout-domestique-170841

But the advocates of AVS don't let reality get in their way and are quick to promote the belief that these systems, along with the cameras they rely on, enhance public safety. This vague and abstract principle is used to sell AVS software, which can be used in various ways according to the whims of law enforcement and current priorities. For example, there is already a political demand for AVS specifically designed to detect joyriding or hawkers.

B Transforming Police Practices

Algorithms for AVS systems are designed to be used by law enforcement agencies, systematizing their repressive and discriminatory logic while further dehumanizing the relationship between the police and the public.

Control-Oriented Society Supercharged With Algorithms

AVS is emblematic of the biopower theorized by Michel Foucault. Security, or what Gilles Deleuze would call "the society of control," functions by steering flows in open environments in real time. After the disciplines that marked the rise of the nation-state and industrial capitalism in the 19th century (and which Foucault summed up in the phrase "make live and let die"), the society of control seeks to regulate flows in real time ("*laisser faire, passer et aller*").*3*

In a context where the power of the State and major capitalist organizations is based on their ability to increase various flows (of people, goods, capital, and data), **social control must be**

3 Regarding the power regimes identified by Foucault, see Olivier Razac, *Avec Foucault, après Foucault : disséquer la société de contrôle, L'Harmattan, 2008. On the concept of biopower in Foucault's work, see in particular Michel Foucault, Sécurité, territoire, population : Cours au Collège de France, 1977-1978, Seuil, 2004, pp. 62-64. Finally, see Gilles Deleuze, 'Post-scriptum sur les sociétés de contrôle," L'Autre journal no. 1, 1990.*

“frictionless” and capable of scaling up to control each of its components “on the fly.” By multiplying calculations, aggregating statistics, and identifying and classifying individuals and their behaviors through largely invisible mechanisms, AVS is one of the most perfect examples of these new modes of police control, the key to the old fantasy of a **“permanent, exhaustive, omnipresent surveillance, capable of making all visible,”** as described by Foucault in *Discipline and Punish*.[4]

However, in the society of control, disciplinary logic still functions at full capacity, with individuals internalizing dominant norms when they feel observed by video surveillance devices. In that it formalizes the norm in its computer code, AVS **pushes the surveillance mechanism to its limit and becomes an excellent tool for normalization**. It then becomes a powerful vector for transforming the way we experience the city.

The Multiplication of Police Forces

Today, the vast majority of what is filmed by cameras is never watched. With nearly a hundred thousand video sensors on public roads, it is neither politically realistic nor economically sustainable to place an agent behind each camera to monitor what is happening in real time. Even Christian Estrosi, mayor of Nice, admits it: “We have 4,500 cameras but we don’t have 4,500 operators. A signal is needed to indicate where something is happening.”[5]
In Marseille, in documents related to the public contracts for the experimentation of automated video surveillance, the city indicated in 2018 that “*its operators cannot monitor all the feeds*” and that “*it is therefore needed for the software to allow for autonomous visualization.*”[6]

4 Michel Foucault, *Surveiller et punir, Naissance de la prison, Gallimard, 1975, p. 215.*

5 “Caméras augmentées : en première ligne, Nice veut « aller beaucoup plus loin »,” *La Croix, April 2024,* https://www.la-croix.com/cameras-augmentees-en-premiere-ligne-nice veut-aller-beaucoup-plus-loin-20240412.

6 “Programme Fonctionnel Technique final - Acquisition d’un Dispositif de Vidéoprotection Intelligente”, 2018, https://data.technopolice.fr/fr/entity/fs2gpylqvgs.

AVS addresses a **political economy problem** *related to video surveillance,* **ensuring that no image escapes a now automated police analysis***. For example, tracking political opponents or a predetermined group used to require significant human resources, forcing the police to prioritize cases. Today,* **AVS eliminates these human and material constraints***. Through automation, any agent can now follow, at almost no cost, the activities of a person or group of people on all cameras in one or more cities, or with drones, in real time or in delayed mode.*
In a police investigation, watching video recordings in delayed mode to find clues or evidence takes a considerable amount of time, requiring several officers for long hours of work. For instance, this was the case in the investigation of the "Lafarge" affair, following an action by environmental activists in the multinational cement company's factories: investigators exploited a large quantity of video surveillance images to find material elements supporting their version.[7] With AVS in delayed mode, which allows for the search of certain elements using keywords and offers the possibility of condensing long hours of recording, **many images that were previously not exploited can now be analyzed with a single click**.

In the long run, AVS makes **systematic detection of offenses** possible. Following the automated speed radars designed to repress speeding, AVS allows for the **automation of "video ticketing,"** generating an untapped source of revenue for public authorities. In some cities, alerts are already being produced by AVS systems to punish certain traffic violations. Operators simply need to review the alerts to issue a ticket and impose fines.[8]
If police files were linked to these systems, it would become relatively easy to identify individuals through facial recognition and expand the scope of offenses.

7 "Affaire Lafarge. Les moyens d'enquête utilisés et quelques attentions à en tirer", article published on *Rebellyon, available at* https://rebellyon.info/Affaire-Lafarge-Les moyens-d-enquete-25197.

8 Thomas Jusquiame, "Les cuisines de la surveillance automatisée," *Le Monde diplomatique, February 1*st, 2023.

With AVS, the current 250,000 police officers and gendarmes can reach the capabilities of millions of agents who do not use these technologies. This could lead to **a police-to-population ratio typical of police states**, without any effective counter-power being established.

Dehumanization and Automation Biases

AVS systems encode **a stereotypical view of "criminality" and "suspicious" behaviors or individuals** into a technical device. The algorithm's code is fixed, lacking nuance. By generating alerts that prompt the officer to act, it overrides any human assessment of a given situation.

The role of the human operator, who decides on the follow-up actions for the alerts generated by AVS systems, is presented as a guarantee by the proponents of techno-policing. The argument is that the presence of a police officer at the end of the chain compensates for the algorithm's rigidity. However, this overlooks the **"automation bias"** that leads humans to **put excessive trust in algorithmic systems**. In practice, the use of an algorithm risks taking even more responsibility away from police officers. It gives them a false sense of control and provides a convenient alibi ("The machine said so!") for justifying their intervention in a specific place or time.

By integrating AVS technologies into their decision-making process, **the distance between the police and the population grows**. This distance is **physical**: the police-citizen relationship is increasingly mediated by technological devices. This is the paradigm of "connected" or "augmented" officers, equipped with body cameras, tablets, and smartphones with automatic license plate reading software and apps to access police files. It is also due to the "robocopization" of equipment, the culture of armament, and systematic car patrols, which contribute to creating a bigger distance between the police and residents.

Video surveillance and the additional algorithmic layer induced by AVS exacerbate these trends: in their daily activities, officers are no longer on the streets, but behind their screens, most often in a control room, the USC, from where they observe the population from afar. And when they do intervene, it is to arrest and abuse. AVS contributes to worsening these dynamics.

The distance is also **intellectual: these augmented police officers no longer need to understand, contextualize, evaluate, or anticipate the actions of other humans when a machine does it for them**. AVS systems encode a stereotypical view of "criminality" and "suspicious" behaviors or individuals into a technical device. By generating alerts that prompt the officer to act, it overrides any human assessment of a given situation.

C

A city where bodies are controlled

AVS encodes a specific view of behavioral norms and deviance into its algorithms, a law enforcement perspective that is scaled up through its implementation in algorithms. In doing so, it runs the risk of **reinforcing the exclusion and stigmatization of those who are perceived as suspicious or illegitimate users of the public space**.

We are all under suspicion: arbitrary police decisions turned into algorithms

Real-time algorithmic video surveillance aims to automate the task of monitoring surveillance videos. It asks the software to look for anything that seems "unusual." In practice, this means identifying "odd" individuals or "abnormal behaviors" through "weak signals." **These "weak signals" supposedly help identify "suspicious" persons who** *may have committed* **or** *who might be capable of committing* **an offense**, thereby systematizing and automating arbitrary criteria already used by the police. Physical or behavioral characteristics that are already perceived as suspicious, often unjustly discriminatory, racist, or stigmatizing, will end up being "encoded" into video surveillance algorithms. In the process, completely ordinary situations can be labeled as "suspicious" and worthy of police attention. In reality, **no behavior is inherently suspicious**; it only becomes suspicious in relation to a particular representation or view of society.

Behaviors Identified by AVS

Concrete examples of AVS in France show that the behaviors that can trigger an alert are quite mundane. For instance, the Jaguar software developed by the Evitech company identifies "frequent stops," "contrary motion," "groups," or "insufficient or excessive speed" as suspicious behaviors. In Vannes, the Cogitech company won the public contract for AVS. The associated technical document stipulates that the software analysis should cover the following behavioral data: "walking, running, standing, sitting, bending down, crouching, etc."

The city cleaned of its "pests"[9]

The list of situations detected by AVS systems clearly illustrates the **uses of public space that are perceived as legitimate, and those that are instead demonized, hunted down, and repressed**—the "pests," the term used by police unions in response to the murder of Nahel and the uprisings in working-class neighborhoods sparked by the tragedy.

For example, one documented use of AVS is to detect "loitering," which means a person who remains stationary for too long or limits their movements to a restricted area. AVS also looks for people on the ground or lying down. **The people who are openly stigmatized by these use cases are beggars or homeless people.** With these criteria, AVS also targets people who work on the streets, such as sex workers. Another use case of AVS is the detection of gatherings of people, especially in front of building entrances. Young people from working-class neighborhoods who

9 The term "*nuisibles*" ("pests") was used in a press release from the Alliance and UNSA Police unions
published on June 30, 2023, following the urban uprisings in reaction to Nahel's murder.

gather on the streets, in part because they do not always have the means to meet in a private space—let alone a quality private space to build social ties—are openly targeted.

AVS further reinforces the repression of activities, behaviors, and lifestyles that are already subject to significant discrimination and police repression. It encodes a stereotypical view of "delinquency" and "suspicious" individuals or behaviors into technical measures. It reinforces **a vision of the street as a transitory space**, a place to pass through rather than a place to live in, a means of getting from one private (preferably commercial) space to another. Individuals identified by the software are those who do not fit into the flow of the city (which should be commuting from home to work and back), those who do not merely move from point A to point B. This approach fuels a utilitarian view of urban life. In short, it targets those who do not participate at all, do not participate enough, or do not participate in the right way in the capitalist machine. One does not sleep on the street, play on the street, or gather on the street. On the street, one is in motion, on one's way.

Such a philosophy was already apparent in the restrictions put in place during the lockdowns due to the COVID-19 pandemic in 2020 and 2021. In France, the lockdown waiver authorized leaving one's home for a defined list of uses deemed "legitimate." Going to work or to school, shopping, and traveling for health reasons. Behind these seemingly harmless choices lies a worldview: that of productive work and consumption.

Our Bodies in Data

Despite the claims of its advocates, **AVS is based on the exploitation of our personal and biometric data**. The manufacturers of this technology view our bodies as a source of information to exploit, providing states with new means for the surveillance of the population.

AVS algorithms are not magical tools. They simply apply a series of instructions. Contrary to what the term "artificial intelligence" might suggest, the machine does not "see," nor does it make a conscious distinction between a human, a trash can, or a car. **For the algorithm, there are only images made up of a certain number of pixels of different colors.** Its creators must use methods to help it detect a pattern—that is, a mathematical combination between the positions of pixels relative to each other and their color—and give it a specific tag (for example, "car," "human," "suitcase," "trash"). **The software only establishes a correspondence between this digital pattern and the words "car" or "human,"** or more precise categories like "human with a red shirt and blue pants."

However, unlike the machine, the law distinguishes between the data that make up the pattern of an object and those that make up the pattern of a human. According to the European General Data Protection Regulation (GDPR), **biometric data** includes **all physical, physiological, or behavioral data that can uniquely identify a person**. These data are considered sensitive and benefit from special protection.

The proponents of AVS attempt to deny the biometric nature of the data processed by their systems in order to elude the protections provided by law. However, even without resorting to facial recognition, **several AVS methods allow for the tracking of a person**—for example, through the color of their clothes or their gait—as they move through urban space and pass through the field of vision of different cameras (this tracking ability is based on so-called re-identification algorithms). If AVS algorithms allow for the re-identification of a person among others based on physical or behavioral data, it is a matter of **biometric identification**.

Biometric identification

Biometric identification is a **technique** used to identify **an individual** from **a group of people** based on their **physical, physiological, or behavioral characteristics**.

Technique to identify an individual	**Sample**	**Characteristics**
facial recognition algorithms	the whole population	distance between certain facial features (keypoints)
re-identification algorithms	individuals present in a given perimeter at a given time	their height, skin and hair color, clothes...

Understanding facial recognition algorithms and their uses

Les algorithmes de reconnaissance faciale ont été « légalisés » en 2012 via le décret à l'origine de la création du fichier de police de traitement des antécédents judiciaires (TAJ). Ce fichier concerne toutes les personnes mises en cause par la police. Le décret prévoit que ces fiches puissent contenir *« la photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale ».*

Les algorithmes de reconnaissance faciale fonctionnent en **attribuant une empreinte à chaque visage**. Cette empreinte est construite à partir de la distance qui sépare certains points du visage, choisis stratégiquement pour garantir que la combinaison des distances permette d'identifier un visage sur une photo avec une marge d'erreur suffisamment faible.

Ainsi, quand la police questionne le logiciel de reconnaissance faciale, elle envoie la photo d'une personne non identifiée, trouvée par exemple sur des images de vidéosurveillance, et **le logiciel compare l'empreinte de son visage aux empreintes des 8 millions de personnes ayant une fiche avec photo dans le TAJ**.

Understanding re-identification algorithms and their uses

Re-identification algorithms allow for the tracking of an individual across multiple images using their physical and behavioral attributes. These algorithms work differently from facial recognition algorithms, as identification is not based on a comparison between a database and an external image, but rather by comparing two surveillance camera images (from different cameras or different times on the same camera) to connect them and retrace the individual's path. **The software creates a "signature" of the person based on many characteristics**, such as the type and color of clothing, silhouette, height, skin color, accessories, and more.

These algorithms are completely illegal but are already in widespread use. They are used in a European project called "Prevent PCP," which is deployed in Paris and Marseille to track luggage from one camera to another. To ensure that it is the same luggage, information about the person carrying it is used. For example, while two bags can look similar, the person carrying them, such as a woman with a red shirt, has unique characteristics that can help identify the luggage. To track a bag, the human who accompanies it and all of their biometric data are used. The term "luggage tracking" obfuscates the fact that ultimately, it is the human who is being tracked.

Loss of Freedom for All

Cities, and public spaces in general, are precious places. They are dense, diverse, and constantly in motion. Many freedoms are exercised there, and one can break free from certain assigned roles. **Anonymity and privacy are fundamental in these spaces.** It is through them that all other freedoms can be exercised: **the freedom to protest, the freedom of movement, the freedom of expression**. However, by strengthening surveillance measures and increasing the number of cameras to add analysis algorithms, **the State is making the violation of privacy a principle rather than an exception**. It operates under the assumption that every citizen is a potential suspect, and that citizens must justify any deviant behavior or their mere presence in certain places. **AVS is fundamentally at odds with the defense of democratic forms of life.**

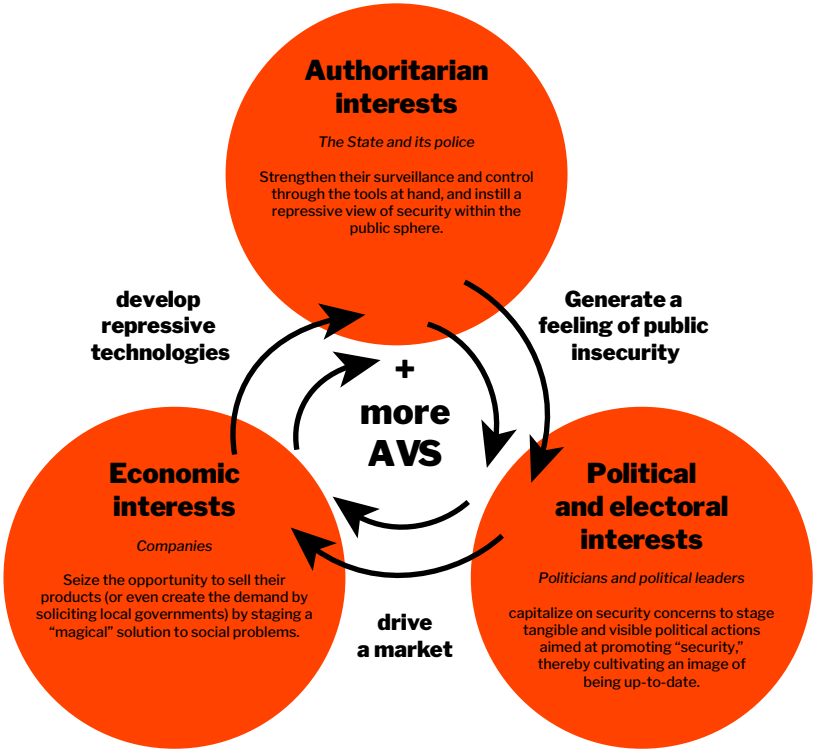
II

The AVS empire

In just a few years, **AVS has become a significant part of public debate and police practice** in France, to the point that it has been the subject of specific legislation within the “experimental” framework of the law relating to the Olympics, which was passed in 2023. To understand this rapid rise, it is necessary to examine the makeup of the networks of actors dedicated to promoting AVS, as well as the **mechanisms of opacity and strategies of acceptability** that they have deployed in order to impose it.

A Converging interests

The deployment of AVS does not meet any truly documented societal need, but instead results from a convergence of interests: **an economical** one for the companies that develop it, **a political and electoral** one for policymakers, and **an authoritarian** one for law enforcement, as it continually increases its power of control.



Economic interests first

Private companies sell video surveillance software to cities, local authorities, and other private entities, such as businesses. This new commercial **"offering,"** focused on the automation of video surveillance analysis, is part of a larger phenomenon: **the security market**. This is a highly profitable and rapidly growing sector, estimated at **34 billion euros in France (1.6% of GDP)**.[10] Within this thriving sector, the **video surveillance business** is particularly strong, with the CNIL[11] estimating that the industry's revenue reached **1.7 billion euros in 2022**.[12]

Globally, the private security market is estimated at 660 billion euros and the video surveillance market at 45 billion in 2020 (with projections of 76 billion for 2025). AVS represented more than 11 billion dollars in 2020 worldwide, with a growth rate of 7% per year.[13]

As sociologist Myrtille Picaud shows in her research,[14] the digital market for urban security is invested by **a diverse range of actors**:

* Firstly, by large **multinational corporations in the tech sector**, such as IBM in Toulouse, which equipped around thirty cameras in the urban area with automated video surveillance software.
* Secondly, by **security industry players** who have been supported by public subsidies and have taken an interest in the

10 Myrtille Picaud, "Peur sur la ville. La sécurité numérique pour l'espace urbain en France," Research Report, École urbaine de Sciences-Po, 2021, https://hal.science/halshs-03138381.

11 *Commission nationale de l'informatique et des libertés, National Commission on Informatics and Liberty.* It is in charge of insuring that data privacy law is applied to the collection, storage, and use of personal data.

12 Philippe Gosselin and Philippe Latombe, "Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité," Assemblée Nationale, April 2023, https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information.

13 "Ce que pèse le marché mondial de la surveillance," *TelQuel, July 2021, https://telquel.ma/2021/07/02/ce-que-pese-le-marche-mondial-de-la-videosurveillance_1727755.*

14 Myrtille Picaud, "Peur sur la ville. La sécurité numérique pour l'espace urbain en France," Research Report, École urbaine de Sciences-Po, 2021, https://hal.science/halshs-03138381.

digitization of this market. For example, Thales with the Safe City experiment in Nice and La Défense, or SNEF in Marseille.
* Smaller and more recent **startups** have also been launched to position themselves in this promising market. Some explicitly target the urban police market, like Videtics, a startup based in the Sophia Antipolis technology park near Nice. Others try to create a more virtuous and "ethical" image, like the XXII company which, after losing several security contracts, now primarily emphasizes seemingly harmless uses (such as automatically detecting the arrival of a pedestrian to turn traffic lights red for cars).[15]
* Finally, **foreign companies** large and small are also present. One of the most widely used video surveillance software solutions in France is developed by Briefcam, an Israeli company owned by the Japanese group Canon:[16] as many as 200 French cities are said to be equipped with its AVS technology.[17]

Money attracts money, and **major groups and startups in the sector are raising funds, both from public actors (such as BPIfrance) and private investors**. The government also subsidizes these companies for **research funding**. For example, in 2019, the ANR (*Agence Nationale de la Recherche*, National Research Agency) granted more than one million euros to Idemia, Thales, and Deveryware (since acquired by the surveillance specialist holding company ChapsVision) to develop AVS applications in conjunction with the Paris prefecture of police.[18]

By running their algorithms on video surveillance feeds, **these companies aggregate large amounts of personal and biometric data** for analysis, exploitation, and cross-referencing to train and **develop software that will be sold on the international market**. Furthermore, for real-time AVS, these companies define what "normal" or "abnormal" is within public space.

---

15 This startup entered into a partnership with the city of Suresnes in 2021 and directly used the city's cameras to train its algorithms, with the city's residents transformed into guinea pigs for the commercial development of a surveillance product. Read the analysis here: https://technopolice.fr/blog/les suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/.

16 More information on this company here: https://technopolice.fr/briefcam/.

17 Thomas Jusquiame, "Les cuisines de la surveillance automatisée," *Le Monde diplomatique, February 1st 2023: https://www.monde-diplomatique.fr/2023/02/*JUSQUIAME/65535.

18 See the presentation of the S^{2}UCRE (Safety and Security of Urban Crowded Environments) project here: https://data.technopolice.fr/fr/entity/dd33j6ttis?page=2.

Focus on One of the Companies Selected for the Olympic Games

Among the companies selected for AVS trials for the Olympics, Parisian startup Wintics is a notable contender. Founded in 2017, Wintics is a major player in the market with its Cityvision software, which offers crowd analysis, detection of "suspicious presences," and identification of "violent or dangerous behavior on train platforms." The solution has been used in RATP train stations and on the Tour de France for bicycle counting, and was recently installed at Rome's airport for "flow management." Wintics' founders have frequent public appearances with the government and represent France in international trade shows. The company is one of the businesses chosen to implement the AVS trial in transportation as part of the Olympics law (see Part III).

Electoral Interests

AVS fits perfectly into the mechanism of activating a sense of concern for public security. Like video surveillance before it, AVS is presented as **a technological solution available to mayors who want to give the illusion of taking concrete action against crime or public disorder**.

The political appeal of AVS also stems from the supposedly "innovative" and "smart" nature of digital technology. Detection algorithms represent innovation and an allegedly "inevitable" future. Many political leaders, including those from small communities, want to adopt them **to project an image of progress and modernity**.
Therefore, like cameras, AVS relies on **techno-solutionism**. It claims to solve a political problem at a lower cost, while justifying the existence of the already installed fleet of cameras.

Authoritarian Interests

Finally, as previously mentioned, video surveillance considerably amplifies the power of control and surveillance of the police. **By adding automatic and continuous analysis of video feeds, law enforcement agencies can significantly increase their surveillance activities, interventions, fines** *via* **video, and arrests.** This also allows them to constantly compile information about our presence in public spaces, including behavior, movements, and habits. The data collected from these automated processes give the police even more power to intrude into our lives, contributing to the authoritarian trend that is becoming increasingly apparent.

Given this convergence of economic, political, and authoritarian interests, it's clear how video surveillance has been able to develop so quickly and easily, with each interest fueling the others. Surveillance companies have found their purpose by tapping into the reactionary discourse on crime that has been perpetuated for years. Their technology has been marketed as an innovative solution to public order concerns. Politicians, both at the national and local levels, have embraced it for electoral purposes. Finally, the police have been reinforced in their central role in social regulation and control.

This **techno-security approach** ultimately contributes to activating the fear of a portion of the population, further fueling the social demand for video surveillance. This is especially true given that all institutional safeguards meant to protect human rights are being undermined by several layers of opacity.

B

A Hidden Advance

While the dangers of facial recognition have been a hot topic in the public imagination, other applications of AVS remain unknown to most of the population. Even for those who take an interest in the subject, **it can be difficult to understand how AVS is developed** or what its range of uses entails. It is **even more challenging to determine which of these uses are currently being employed by law enforcement**. By maintaining this opacity, promoters of AVS, such as political leaders and corporations, attempt to deploy the technology. Once it is in place, it is usually too late to reverse its implementation. **The opacity surrounding AVS has become an obstacle to the exercise of democratic mechanisms and political opposition.**

Political and Administrative Opacity

The use of AVS by law enforcement for investigative purposes is already in effect, with **deployment primarily happening at the local level**. This is because it is typically local authorities (municipalities, regions, etc.) that manage video surveillance systems and have the authority to implement AVS software. Despite the fact that this technology is entirely illegal, regardless of its use cases, it has been able to proliferate across France based on scattered and geographically dispersed decisions made by cities that are often unconcerned with the legality of these systems, receptive to commercial spiels from corporations, and responsive to requests from municipal police services.

This expanding network of local authorities using AVS has contributed to **establishing a** *de facto* **situation at the national level, effectively introducing and legitimizing the surveillance technology despite its complete illegality**.
Decisions to invest in surveillance software are usually made during municipal, departmental, or regional council meetings and are recorded in the minutes of these sessions. In most cases, the authority issues a call for tenders to acquire and install a software solution, to which AVS companies respond. These documents, including minutes and calls for tenders, are administrative documents that are not typically made public but that can be accessed by anyone making a request in accordance with certain legal provisions. This process, known as a "CADA request" (named after the *Commission d'accès aux documents administratifs*, Commission for Access to Administrative Documents), **allows anyone to request access to a public document** via email or physical mail, provided they follow a specific format.[19]

If the administration does not respond within two months, it is possible to bring the matter to the Commission for Access to Administrative Documents to enforce the request. While the CADA request method can be uncertain (documents provided are often redacted or incomplete) and time-consuming, **it remains the most effective method for lifting the veil of secrecy surrounding the deployment of AVS software**.

19 See our guide on how to make CADA requests: https://technopolice.fr/blog/guide se-renseigner-sur-la-surveillance-dans-sa-ville/.

Briefcam in Moirans

The town of Moirans, in the Isère department, has decided to implement the AVS software developed by Briefcam. La Quadrature du Net made a CADA request to the town for the user manual. However, the town refused, citing that they were not allowed to disclose it due to trade secret protections. La Quadrature then had to appeal to the Commission for Access to Administrative Documents, which ruled that the manual was indeed communicable under French law. Despite this, the town still refused to disclose the document, forcing La Quadrature to file a lawsuit. When the case reached the administrative tribunal, the town of Moirans ultimately dropped the case and disclosed the document without waiting for a judicial decision, which would have likely been unfavorable to them.

CADA ruling available here: https://cada.data.gouv.fr/20212725/.

The decision to use AVS is often not made public and is imposed on the residents of towns without their consent. This technology is highly intrusive and significantly impacts the exercise of their freedoms and how they experience their city. There is typically no debate or vote held among the community to decide whether to implement such surveillance technology. Even opposition politicians often face **a lack of transparency**. Furthermore, once these software systems are installed, **no information is provided to the individuals subjected to algorithmic analysis**. As a result, people are unaware that they are being analyzed by a video surveillance camera.

When the public is kept in the dark about these projects, the democratic mechanisms for contesting them and the legal safeguards that would normally apply cannot be mobilized to oppose AVS.

Technical opacity

The algorithms used in AVS are developed by private companies that have complete control over the choices in the code. **These choices often include political decisions.** Increasing transparency throughout the development of these algorithms would at least allow for a better understanding of how these choices are made.

AVS software combines various computer vision algorithms, including:

- **Detection** algorithms, which isolate different elements of an image
- **Identification** algorithms, which classify these elements
- **Tracking** algorithms, which track these elements
- **Facial recognition** algorithms
- **Line-crossing** algorithms, which detect when an element is in a certain area of the image
- And many other algorithms that, when combined, offer a wide range of analysis.

The extent of a software's capabilities is determined by the company, often based on the demands of local governments or the police, by combining these different algorithms. **The software code is never published, nor are the choices of which algorithms and settings are used, or the datasets used to train the identification algorithms. The entire production chain is opaque**, making it impossible to know what specific biometric data AVS is processing.

Some of these algorithms use a subcategory of machine learning called deep learning. The unique aspect of deep learning is that the variables used in the correlations are hidden under layers of calculations, making them imperceptible. For example, to categorize an image of a cat, the designer does not specify to the algorithm to look for pointed ears or whiskers. Instead,

the algorithm uses any information available, such as the relative position of pixels and their color. The variables used in practice may not even be comprehensible to a human. As a result, there is a "black box" in the algorithm's reasoning that no one can understand. **Deep learning is also opaque regarding the variables used, including for the person who designs and implements it.**

AVS software is used by the state, yet there is no clear public information available about their functioning. During debates on the Olympics law, **the government refused to grant a right to transparency for these algorithms**, citing "security" reasons. The only way to understand how they work is to study commercial communications for the software. However, this information is often loaded with marketing language and is not sufficient to clearly establish what the software's classification operations are.

Practical Opacity

AVS software is a commercial product that follows a supply and demand logic. When addressing potential clients, such as local governments, companies aim to sell their license by highlighting as many "needs" as possible that the software can address. Therefore, a city that decides to implement surveillance for illegal dumping may be offered the "full package" of AVS software, which may include other surveillance uses. The police, using the software, will then have access to multiple tools without it being possible to know exactly which ones are being used in practice. This adds to the **practical opacity of what is actually happening in police stations and urban surveillance centers**.

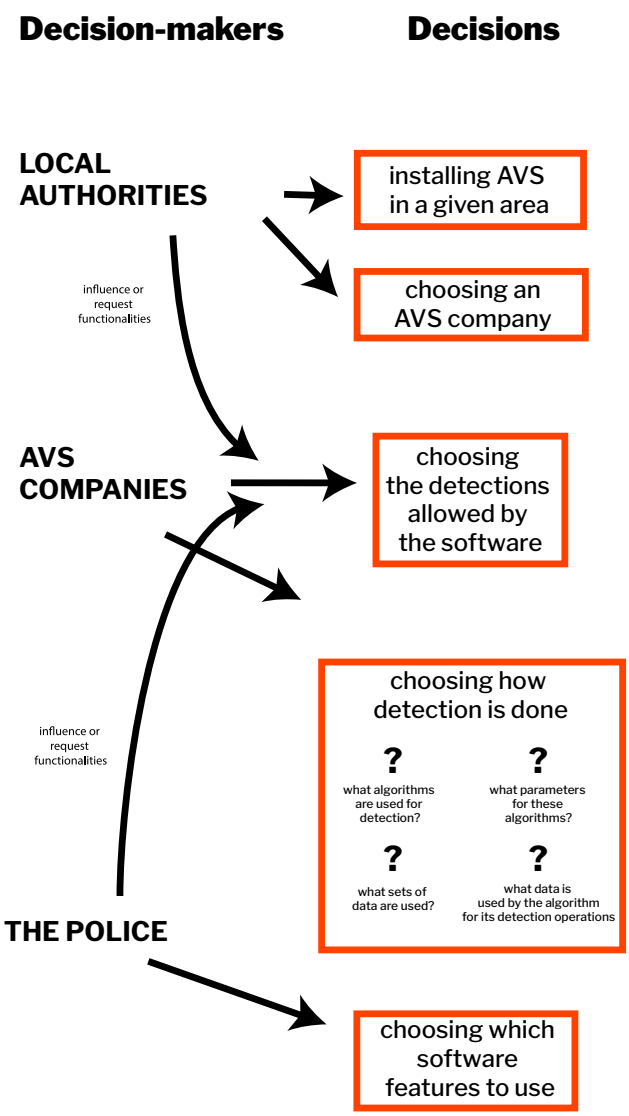
The Example of Marseille

A Marseille, le marché public prévoit une « tranche ferme » et une « tranche conditionnelle », c'est à dire un logiciel de base et une couche supplémentaire à installer ultérieurement, cette dernière contenant les usages les plus problématiques. Il est cependant impossible de savoir si celle-ci a été un jour implémentée. De la même manière, le logiciel Briefcam prévoit une simple case pour activer la reconnaissance faciale, qui d'après des retours du terrain est cochée par défaut. Les commerciaux de l'entreprise n'hésitent d'ailleurs pas à expliquer patiemment à leurs clients comment désactiver l'option en cas de contrôle inopiné de la CNIL.

The claim of establishing technical safeguards and drawing a clear line between acceptable and unacceptable AVS is a pipe dream. "Detecting an object in the middle of the road" and "detecting a person sleeping on the street" are two actions that use the same algorithms, and a technical boundary cannot be established between the two. The practical opacity and lack of scruples of the police assure us of one thing only: **the only safeguard possible is a total ban on AVS**.

Ultimately, **almost no one knows what AVS is**. And if someone knows that AVS exists, they cannot know where it is deployed. If a person is arrested by the police, they will not know whether AVS played a role in their arrest. If they make a CADA request and know that AVS is present in their city, they will not be able to find out its true purpose and will not be able to oppose it.

The implementation of AVS
Where are the decisions made, and by whom?
How can we learn about these decisions?



C

Making AVS Acceptable

In addition to its commercial deployment in cities, **the AVS industry has also taken steps to create a positive image for itself in public discourse**. In order to win over the public and institutions, the sector has employed various strategies to make this surveillance technology acceptable and associated with an aura of respectability.

Pretending Technology Is Neutral

Surveillance technologies are typically presented as simple technical tools with the sole purpose of helping the user in a neutral and impartial way. **However, nothing is neutral when it comes to AVS.** Every technology is shaped by the conditions in which it was developed and the intentions of its creators. At every stage, **AVS reproduces and encodes human decisions and subjective visions of society**, which have significant political consequences.

To convince people and institutions that AVS is a consequence-free software, **the language used to name and describe this technology is a major strategic issue**. The industry has developed a marketing discourse that is both optimistic and minimizing, aimed at **overshadowing the true nature of what is recorded and analyzed by the algorithms**.

We have explained that AVS software analyzes and classifies what is represented in video surveillance images, which are most often human beings. To make correlations, the algorithms will use the data present in these images, i.e., information and characteristics related to bodies and behaviors, or "biometric data." However, the term "biometric" immediately brings to mind issues about privacy and carries strong symbolism as well as intrusive connotations.

In their discourse, companies have therefore made efforts to mask this reality by using semantic games and euphemisms. AVS software is generally presented as analyzing and classifying "objects," even though this categorization includes people.

The AVS industry is aided in this by the academic community. Researchers have recently shown how the computer vision scientific community promotes **a neutral and purely intellectual perception of automated image analysis technologies for humans**. By **separating their research from the applications** that will be made downstream and minimizing the fact that they deal with human data, researchers contribute to **hiding the intrinsic link between the technology and its practical uses, which then become one of the founding layers of the surveillance paradigm**.[20]

By not distinguishing between humans and objects, companies aim to homogenize and equate the data processed in these two categories, even though they are politically and legally very different in their consequences. Using the color of a car to establish correlations does not have the same implications as using a person's skin color. By lumping everything together, **the promoters of AVS avoid any political discussion about the surveillance** of which their software is the instrument.

20 Pratyusha Ria Kalluri, William Agnew, Myra Cheng, Kentrell Owens, Luca Soldaini, and Abeba Birhane, "The Surveillance AI Pipeline," September 2023, <https://arxiv.org/abs/2309.15084?ref=404media.co>.

Le tableau ci-dessous fournit une brève description de chacune des dimensions disponibles :

Nom de la dimension	Description	Exemples de valeurs
Classe	Classe d'objet G	arçon, Fille, Voiture, Camion
Classe (Personnes)	Seules les classes d'objets "Personne", c'est-à-dire : Garçon, Fille, Homme, Femme	Garçon, Fille, Homme, Femme
Classe (Véhicules routiers)	Seules les classes d'objets "Véhicules routiers", c'est-à-dire : Moto, Voiture, Pickup, Fourgonnette, Camion, Bus	Moto, Voiture, Pickup, Fourgonnette, Camion, Bus
Catégorie de classe	Contient les catégories de classe suivantes : Personnes : Garçon, Fille, Homme, Femme Vélos : Vélo Véhicules routiers : Moto, Voiture, Pickup, Fourgonnette, Camion, Bus Autres véhicules : Train, Avion, Bateau	Personnes, Vélos, Véhicules routiers, Autres véhicules
Couleur	Couleur principale de l'objet	Noir, Vert, Orange
Heure de fin de l'objet	Heure de fin de l'objet dans le cadre 1	9/03/2018 13:04:11
Heure de début de l'objet	Heure de début de l'objet dans le cadre 1	9/03/2018 13:00:02
Date	Date de l'objet 1	9/03/2018
Date et Heure	Date et Heure de l'objet 1	9/03/2018 13:03
Jour	Jour de l'objet L	un, Mar, Mer
Jour (numéro)	Numéro du jour de l'objet (par exemple 19 si la date est 19/03/2018)	1,2,15,17,19
Heure	Heure de l'objet dans le format de plage horaire	04:00-05:00, 21:00-22:00
Heure (hh)	Heure de l'objet dans le format heure 0	6:00

In a similar way, the software supposedly focuses not on "behaviors" but on "situations." For instance, the city of Orléans attempted to pass off the algorithmic audio surveillance installed in its streets by the Sensivic company as a simple "air vibration detector."[21] In reality, this technology is based on microphones paired with analysis software that works like AVS and facial recognition, analyzing human activity in order to detect cries or various sounds.

Finally, by attributing any software errors to "biases" and "overrepresented correlations," companies perpetuate the notion that an algorithm can be neutral and can provide an objective analysis of reality. This contributes to the illusion that any software error is solely due to a technical malfunction that can be fixed. However, as previously discussed, all decisions made by the software are political and merely reflect prior human decisions and visions encoded in the algorithm. By insisting that the real decision is made by a person at the end of the chain, AVS promotional discourse (often echoed by institutions) masks, either deliberately or through a lack of technical understanding, all the choices made by manufacturers that influence and guide this decision.

Minimizing the Impact on Liberties

Another strategy involves **associating AVS with other seemingly less problematic technological uses**. For example, they emphasize situations where human activity is least perceptible, such as counting cars, detecting trash on sidewalks, or identifying abandoned luggage. However, this overlooks the fact that the algorithm continuously scans video feeds from the street or public space where the object is located. By using this rhetorical approach, companies avoid clarifying that **human analysis is constant, even when detecting an object**.

21 See our analysis here: https://www.laquadrature.net/2023/01/12/surveillance-sonore orleans-baratine-la-justice/.

In this **minimization logic**, various biometric surveillance tools are often put side by side, to **present some as dangerous for liberties and others as harmless in comparison**. The goal of this strategy is to rank these technologies, stigmatizing some while keeping others shrouded in opacity to hide their severity. With this rhetoric, biometric surveillance companies aim to appear to be establishing a so-called guard rail, projecting an image of concern for liberties, even as they undermine them.

Facial recognition is a strategically useful tool in this context. Widely known and represented in dystopian fiction for a long time, it instantly evokes mass surveillance, symbolizing the "red line" not to be crossed in the collective imagination. Companies are aware of this and attempt to **differentiate facial recognition, which is perceived as dangerous, from other biometric surveillance technologies**, portrayed as less severe and therefore acceptable. Consequently, laws may prohibit facial recognition, presenting it as a protection of privacy, while other AVS use cases that don't rely on facial recognition function similarly and pose the same risks to society.

Seizing Every Opportunity

Any opportunity is exploited to introduce surveillance measures into public discourse. By **activating feelings of anxiety about public order and playing on fears** during special events, technology is presented as a **magical tool** to resolve unprecedented problems. The COVID-19 pandemic, for example, served as a pretext for drone use, movement tracking, and the accelerated collection of health data.

Similarly, **the Paris Olympic Games were instrumental in accelerating the political agenda for the legalization of AVS**.

Major sporting events, due to their exceptional nature and "out-of-time" dimension, enable the implementation and acceleration of equally exceptional policies. Researcher Jules Boykoff compares[22] the legislative acceleration phenomenon to Naomi Klein's "shock doctrine" theory, which describes how governments use disasters or social traumas to implement privatization and deregulation measures where none existed before. Boykoff analyzes the Paris Olympic Games as an accelerator of exceptional policies, this time relying on a festive, spectacular moment, perceived as inherently "extraordinary," where political rules can be temporarily suspended to advance policies that would have been impossible to implement under normal circumstances.

For example, before the Tokyo Olympics in 2021, the Japanese government passed an "anti-conspiracy" law,[23] which had been long awaited by some politicians to suppress activists and labor groups. The legislation faced severe criticism, especially from the United Nations, for violating civil liberties and bestowing excessive surveillance powers on the government. More recently, Qatar has implemented a large-scale surveillance system[24] for people attending the 2022 Football World Cup.

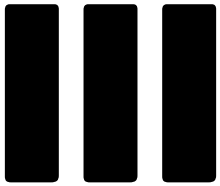
In France, the government used the Paris 2024 Olympics to promote the acceptance of AVS. Gérald Darmanin explicitly stated that "extraordinary situations require extraordinary measures." However, this technology did not change the course of the event in any way, because it required logistical and human support more than anything else. Instead, **the sporting event simply provided an opportunity to accelerate a much broader and long-term political agenda: the establishment of a generalized surveillance empire in public spaces**.

---

22 Jules Boykoff, "Les Jeux Olympiques, le capitalisme de fête et la réponse des activistes", 2019, https://saccage2024.noblogs.org/files/2021/07/boykoff-v5.pdf.

23 Yann Rousseau, "Le Japon adopte une loi sécuritaire controversée," *Les Échos, June 16, 2017, https://www.lesechos.fr/2017/06/le-japon-adopte-une-loi-securitaire-controversee-172489.*

24 Clément Le Foll and Clément Pouré, "Mondial : le Qatar met les supporters et le pays sous étroite surveillance," *Mediapart, November 19, 2022, https://www.mediapart.fr/journal/international/191122/mondial-le-qatar-met-les-supporters-et-le-pays-sous-etroite-surveillance.*



The worst is yet to come

Street surveillance has been in use for over thirty years, starting with the first installations of cameras. However, it has significantly accelerated with the development of biometric surveillance algorithms. The legalization of AVS in the law related to the Paris Olympics which was adopted in 2023 marks a turning point in the security overhaul of public space. Behind the unprecedented legalization of certain AVS uses, other techno-security devices, which have already been illegally experimented with, could also be legalized. Biometric categorization, facial recognition, sensors of all kinds—there is a lot of political demand for the legalization of new surveillance tools, and their implementation may come sooner than we think.

A An age-old political agenda

To understand the place given to AVS in France today, one must look back at the history of its **basic infrastructure: video surveillance**. It appeared in the 1990s and was quickly presented as a techno-solutionist response to fight against "public order concerns."

Financial Overspending

After the creation of a legal framework in 1995 and several controversial local deployments, it was during Nicolas Sarkozy's presidency in the 2000s that the French State took on video surveillance to turn it into a national policy instrument. In 2007, the Interministerial Fund for the Prevention of Delinquency and Radicalization (FIPDR) was created. This fund finances prevention plans, and very soon, its grants to municipalities started being oriented towards the installation of surveillance cameras. Two thirds of the credits were allocated to installation programs between 2010 and 2012.[25] In 2023, 30 million euros were spent on video surveillance projects, doubling the amounts used for this type of project between 2007 and 2009.

25 Philippe Robert and Renée Zauberman, *Du sentiment d'insécurité à l'État sécuritaire (Le Bord de l'eau, 2017), 91.*

This funding has paid off, as the number of cameras has skyrocketed. There were at least **90,000 video surveillance cameras deployed by the police and local communities on public roads alone at the beginning of 2023, to which we can add approximately 50,000 body-worn cameras and 800 police and gendarmerie drones**.[26]

As with any such costly public policy, there should be reliable assessments of the effectiveness or usefulness of video surveillance. However, sociologists Philippe Robert and Renée Zauberman state that "this build-up has been facilitated by the systematic refusal of any real evaluation, hidden behind a pseudo-administrative review that does not respect any of the rules of the genre." Indeed, the **French State refuses to conduct any form of review**, and the few independent studies carried out on the subject all point to the **ineffectiveness and disproportionate cost-benefit ratio of video surveillance**.

Among the few studies that exist, the 2020 *Cour des Comptes* (Court of Accounts, France's supreme audit institution) report[27] notes that "no global correlation has been found between the existence of video protection devices and the level of public space delinquency or clearance rates." Video surveillance is therefore ineffective and useless. However, the authorities refuse to admit it and continue to cite anecdotal evidence or police testimonials indicating that it is crucial for solving cases or preventing delinquency.

26 Philippe Gosselin and Philippe Latombe, "Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité," Assemblée Nationale, April 12, 2023, <https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information>.

27 "Rapport sur les polices municipales," page 70, accessible at https://www.ccomptes.fr/fr/publications/les-polices-municipales.

Industries have taken advantage of this “technological bluff” to offer new products and fuel their business: cameras are not effective because there are not enough of them. More cameras should be scattered throughout the territory, with better image quality, offering a wider field of vision (hence the arrival of 360-degree, pivoting cameras, etc.). **Failure becomes a pretext for persisting in this techno-solutionist approach.** Now, **the automation of video feed analysis is being touted as the ultimate solution**.

AVS is part of this **security headlong rush**. But it results from another dynamic, more discreet and yet much more dangerous: **that of biometrics and the automated analysis of bodies in urban public spaces.**

Biometric Pressure

In the face of civil society opposition, the most politically sensitive AVS uses, particularly facial recognition, have been temporarily set aside in favor of applications seemingly less sensitive for public liberties.

B The "Olympic Games" Law: An Hypocritical Legal Step

A step-by-step strategy has taken shape in France through law n° 2023-380 of May 19, 2023, relating to the 2024 Olympic and Paralympic Games, whose Article 10 provides an experimental framework dedicated to AVS to detect certain behaviors in real time. This constitutes the first step legalizing police use of these technologies. It is also the first law on the subject in the European Union, making France the first Member State to choose to approve and test such a dangerous technology.

An In-depth Look

What does this law provide for exactly? Until March 2025, AVS solutions can be used for any type of "recreational, sporting and cultural event" open to the public and "particularly exposed to risks of acts of terrorism or serious threats to the safety of people." Contrary to what the title of the law might suggest, it is not just about the Olympic Games, far from it: **music festivals and football matches are all events that fall within the scope of this trial**. As an example, the first uses of AVS by the Paris police prefecture took place in April 2024 during a Black Eyed Peas concert and for a match between the PSG and OL football teams.

The AVS algorithms, connected to video surveillance cameras, are deployed in and around these public events, as well as in the surrounding transport networks (train and metro stations). They are supposed to detect, in real time, **eight categories of events**, most of which are not very sensitive in terms of public liberties:

- presence of abandoned objects,
- presence or use of weapons,
- non-compliance by a person or vehicle with the common direction of traffic,
- crossing or presence of a person or vehicle in a prohibited or sensitive area,
- presence of a person on the ground following a fall,
- crowd movement,
- excessive density of people,
- fire outbreaks[28]

An opportunity for the private sector

The AVS systems chosen for these experiments are, unsurprisingly, developed by companies in the private sector. **The Ministry of the Interior acquired the technical solutions from private sector providers** after issuing a public tender.

A market divided into **four geographical lots**, all **won by French companies**: Wintics, Videtics, Chapsvision and Orange Business Service—in partnership with Ipsotek, a subsidiary of Atos (now Eviden). Within the French Ministry of the Interior, a steering committee created for the occasion oversaw the deployment. It was led by Julie Mercier, head of the Directorate of Enterprises and Security and Weapons Partnerships (DEPSA) within the Ministry, which says a lot about the interests at stake. **Promoting "French-style" innovation is an important political objective** that is driving

28 Decree no. 2023-828 of August 28, 2023, on the procedures for implementing algorithmic processing on images collected using video protection systems and cameras installed on aircraft. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048007135.

the French State to work increasingly closely with private actors. The CNIL has made a conscious shift in this direction in recent years. Originally created in the 1970s to act as a counter-power to the State's surveillance capabilities over the population, the French data protection authority has now shifted its focus to helping businesses. For the video surveillance industry, the public contract related to the experimentation allowed by the Olympic Games law appeared highly strategic. Indeed, this market is a unique opportunity for AVS companies to demonstrate the superiority of their products, while refining their models thanks to access to the masses of video surveillance data that are opening up to them in this context.

A Forgone Conclusion for a So-called Assessment

The law relating to the Olympic Games provides, rather originally, an "assessment" of the experiment. Behind this term lies a deception intended to ensure the "social acceptability" of a controversial technology—in this case, AVS. By referring to a temporary, reversible measure that will be evaluated at the end of the trial, the aim is above all to **reassure the general public**.

An evaluation committee has been created to review these "trials."[29] However, it is questionable whether this committee will be able to counter the techno-solutionism at work in this operation to legitimize AVS. This type of experimental approach embodied in France by the Olympic Games law corresponds to a real trend in the regulation of police applications of artificial intelligence, that of "regulatory sandboxes." These derogatory measures allow the State and industry to enact a temporary legal framework to encourage innovation, by lowering the guarantees provided for certain regulations of general interest, notably in environmental matters or for the protection of human rights. **It is therefore not surprising to find them in the AI Act, whose Article 59 allows public and private actors to exempt themselves from personal data laws when this is necessary to "safeguard an important public interest," notably in the field of "public security and health."**

29 Decree no. 2023-939 of October 11, 2023.

C

A Case of Not Seeing the Forest for the Trees

Behind the legal legitimation of a few uses of facial recognition technology through the Olympic Games law, there are actually a whole host of **other existing biometric technologies**. Whether they are already being used illegally or are in development, **they are all part of the security project of controlling public space that the promoters of surveillance want to see**.

These Companies Know How to Do Much More

AVS in real time or on archived images, **people tracking and re-identification** based on physical or behavioral attributes (for example, tracking and finding someone based on the color of their clothes), **emotion recognition, facial recognition, counting and categorizing profiles** or **modes of occupation of public space**: all these **biometric surveillance applications are already available from surveillance companies**. They all rely on the same machine learning technology and are developed by the same engineers, following an identical technical logic. Each of these applications represents just one use case in the range of technical possibilities offered by algorithmic video surveillance.

Scope of AVS uses

Legal AVS

Experiments based on the Olympic law, limited to sport, culture and festive events until March 2025.

Detection of:

- Start of a Fire
- Line crossing
- Moving in the wrong way
- Fallen person
- Carry or usage of a weapon
- Important density of people
- Forgotten luggage
- Crowd movement

Non-human detection:

- animals
- vehicules
- licence plate reading

AVS Illegally put in use

Detecting and following people:

- by facial recognition
- by physical characteristics
- being static (used to find homeless people, people asking for money, sex workers, lookouts, loitering..)
- exceeding a certain number of people
- moving too fast or, not fast enough
- showing a certain emotion
- painting a graffiti
- stealing
- deteriorating
- in a given position (knealing, squatting ...)
- wearing a mask
- leaving trash behind
- having an abnormal behavior

in 2024

Uncomplete list of applications detected by the different Technopolice local groups

Finding someone and recreating their path:

- by facial recognition
- by skin color
- by it's cloths and it's colors
- by it's hair cut and their color
- by it's accessories
- by it's gender
- by it's age

Finding and recreating a car's path:

- by it's model and color
- it's licence plate (even part of it)

Other features:

- selective summary of videos (removing moments on inactivity or in large number of images)

Potential uses of AVS

Haven't been found in the study did by Technopolice local groups but technically possible:

Detection and surveillance of people :

- Playing ball
- Putting up posters
- Distributing leaflets
- Wearing a veil
- unaccompanied minors (for example after a curfew)
- drinking alcohol
- staggering (to find drunk people)

Several French AVS companies already offer facial recognition applications, including Idemia, Thales, Axis, Avigilon and Two-I. For now, these are only available in countries that are less concerned with protecting liberties. One company, Ipsotek, a subsidiary of Atos-Eviden, was selected for the public procurement contract linked to the Paris Olympics law, and also developed a real-time facial recognition system and equipped the Abu Dhabi Airport in the United Arab Emirates. According to its website, Ipsotek's VIFace system uses over 300 cameras to identify individuals on surveillance lists and assist law enforcement in tracking them.[30]

As we illustrated earlier (see p. fixme), **facial recognition** is already one of the functions activated by default **in the Briefcam software sold to French police forces**.[31]

As for Two-I, a startup specialized in AVS, it initially focused on emotion detection, which it tested in gendarmeries and attempted to use in trams in Nice, before experimenting with facial recognition on football fans in Metz. The company has since shifted its focus to less sensitive applications, such as statistical counting, under the guise of developing "smart cities." This highlights the fact that **the eight uses regulated by the 2023 law are almost anecdotal compared to the scope of current practices**.

A Legalization Plan Already Underway: The AI Act

The technologies are already in place, but they lack a legal framework and social acceptance to become standard police practices. This is exactly what institutions and politicians are currently working to establish.

The European stage is also a key battleground in this debate.

30 See ATOS, https://archive.ph/YKhJF. See also Ipsotek, "Consumer Stories," https://archive.ph/wip/gaNQ6.

31 According to Disclose, "the facial recognition function is enabled by default" in Briefcam since the release of version 5.2 of the software in 2018. See Clément Le Foll, "Reconnaissance faciale : Gérald Darmanin veut enterrer 'l'affaire Briefcam,'" *Disclose, https://disclose.ngo/fr/article/reconnaissance-faciale-gerald-darmanin-veut-enterrer-laffaire-briefcam.*

The French government has been actively lobbying in Brussels to create a favorable legal environment for the use of AVS and facial recognition. The EU's AI Act has become a focal point for this effort. Initially, it seemed that the EU's risk-based approach to regulating AI might lead to a ban on the most hazardous applications, such as facial recognition. This was the hope of many NGOs and over 250,000 European citizens who joined the Reclaim Your Face coalition. However, France and other states have worked to undermine this goal, effectively **giving law enforcement and the surveillance industry a free hand**.

A closer examination of the text reveals that the regulations are not as restrictive as they initially seem. Article 5, which lists the various prohibitions, does indeed ban the use of real-time biometric identification systems. **Article 5.2 appears to cover many AVS use cases**. However, there are significant loopholes. For one, any use of these systems that is conducted in a delayed manner is exempt from this provision. Furthermore, **exceptions drastically reduce the scope of the ban**. For instance, real-time facial recognition will be permitted in cases where it is used to locate victims of human trafficking, as well as to prevent a specific, substantial, and imminent threat to the life or physical safety of individuals. It will also be allowed to prevent a real and actual or predictable terrorist attack, and in the context of criminal investigations to track down suspects of a wide range of offenses punishable by more than four years in prison, including sabotage, organized crime, murder, and many others. These exceptions effectively leave the door open for further expansion of these measures in the future.

Moreover, the **military and intelligence services are exempt from any constraints** in this regard. The same applies to scientific research teams, which will be able to "innovate" freely. Article 2.3, which defines the scope of the regulation, specifies that it, and therefore the prohibitions it contains, does not apply to AI systems developed "for scientific research purposes" or those used "for military, defense, or national security purposes." This creates yet another significant loophole.

In reality, the regulation seems to allow all forms of police AI that we are opposing in the Technopolice project, including AVS and predictive policing. These systems may be classified as "high-risk" due to their sensitive nature, but this classification would only lead to **additional transparency and standardization requirements**. The responsible parties will have to identify, assess, and mitigate "reasonably foreseeable risks (…) to health, safety, or fundamental rights" (Article 9.2), implement good data governance practices (Article 10), and maintain records of their systems' activities (Article 12). Standardization and self-regulation, under the supervision of public agencies responsible for organizing the whole process, will be the norm.

Transparency for high-risk systems in the context of technopolicing will remain severely limited. Law enforcement and immigration services got exemptions from public registration requirements (Articles 49.4 and 71), and they will also be exempt from publishing impact assessments, which are typically required for high-risk systems.

Even when high-risk systems are identified, **they may still be exempt from regulations due to a loophole**. A "filter" defined in Article 6.3 states that specific obligations do not apply if the AI systems in question are designed to perform a narrow procedural task, improve or optimize a human task, or carry out a preparatory task. Additionally, if the system is deemed not to pose a significant risk to health, safety, or fundamental rights, it may also be exempt. These legal concepts are quite broad and open to abuse, particularly since they are left to the discretion of private actors.

Predictive policing systems that use risk scores based on geographic areas, which we recently highlighted as being discriminatory, appear to fall outside the narrow definition of high-risk systems proposed in Annex III. As a result, they would not be subject to the obligations and regulations intended for this category.

Bogus Safeguards

Far from protecting fundamental rights, the AI Act amounts to the deregulation of police surveillance technologies such as AVS in European Union countries. Proponents of AVS will argue that these tools are indispensable, that they must be used in a regulated manner, and that it is possible to include safeguards in the law to protect rights and freedoms, and that the AI Act can contribute to this. However, **the history of surveillance technologies shows that legal guarantees are systematically ignored**, set aside, or openly disregarded, without institutional checks and balances, such as judges or data protection authorities, being able to enforce them.

The deployment of AVS is a prime example of this. It has been **illegally installed over the years**, and it is clear that neither impact assessments, nor the powers of regulatory authorities, nor the so-called local checks and balances, such as video surveillance ethics committees, nor the public's right to information, have been of any use. What prevails instead is **a sense of total impunity among those responsible**.

To summarize, in France, a **hypocritical government** touts the "highly regulated" nature of the experimental system provided by the Olympic Games law, while condoning the illegal use of Briefcam's AVS software by the national police, **promoting other surveillance technologies**, and already preparing for the future. **Municipalities that have been using illegal software for years** are keeping a low profile while awaiting legislative developments. The incompetence and bad faith of lawmakers, who make no effort to understand the technologies they are legalizing, are **driven by a sensationalist discourse on "public order concerns."** The **CNIL's** cowardice, instead of putting a stop to this surveillance dynamic, **contributes to creating an "ethical" veneer over these technologies**, by creating the illusion of being a sufficient safeguard. Finally, the bad faith—or rather, **the lies—of the surveillance-industrial complex**, which is maneuvering to **turn the streets into a commercial playground**, thereby undermining the possibility of democratic forms of life and **contributing to the rise of authoritarian and repressive societies**.

The only way to keep public spaces free, to avoid increasing discrimination against vulnerable and marginalized individuals, and to prevent the reinforcement of police surveillance power and the legitimation of its violence is to completely ban the use of algorithms to analyze human activities for police purposes. This means that, without a determined mobilization to block this trend, the normalization of algorithmic video surveillance of public spaces is a fait accompli, and its perpetuation and legalization seem like mere formalities.

IV

Fighting Back

Beyond the experiments, **the surveillance world is building its empire**. Having paved the way in politics and structured the economic landscape, the legalization of AVS in the Paris 2024 Olympics law is the first institutional milestone in a historic shift towards permanent and automated surveillance of our behavior in urban public spaces.

We must continue to **express our rejection of this authoritarian project** and remind everybody that the city is ours and that it is a space of freedom. This can involve multiple paths of action[32]: **exposing companies and politicians promoting AVS**, **making the cameras visible**, **demanding accountability from our mayors and lawmakers**, **organizing locally**, **being creative and reclaiming public space together to assert our right to a free city**.

We can act to prevent total surveillance from spreading in our streets.

32 We had already suggested some courses of action against video surveillance in this guide, published in 2022: https://technopolice.fr/guide-videosurveillance.pdf.

A Documenting

One of the main drivers of technopolicing is that it is built and developed in complete opacity. **To counter the AVS projects**, it is therefore necessary to make them visible, understand their features, and reveal how they work. By materializing their existence, we can shed light on the political decisions behind them and more clearly identify the technology we are trying to combat.

Making digital technologies and infrastructure visible is an essential first step towards collective awareness and a useful way to mobilize.

Requests for access to administrative documents are an effective tool available to everyone to obtain information on surveillance systems in a city. Despite their practical and legal limitations, CADA requests remain an effective lever for bringing surveillance projects out of municipal council chambers where they are decided. Since the beginning of the Technopolice project, this right to administrative documents has allowed us to obtain public contract documents, user manuals, camera location maps, etc. To make a CADA request, you can follow the dedicated guide.[33] We also invite you to use the MaDada platform to centralize, track, and share the different requests you have made.[34]

33 You can find it here: https://technopolice.fr/blog/guide-se-renseigner-sur-la-surveillance-dans-sa ville/.

34 To do so, you can create an account on https://madada.fr/.

There are many more ways to document and gather information. Some are already well established and others are yet to be invented. For example, searching for publicly available information on the websites of surveillance companies or local authorities can often lead to detailed descriptions of technologies or case studies of deployments in certain cities. You can also delve into reading minutes of municipal council meetings or attend public meetings. Confronting your mayor or other decision-makers—including lawmakers who will have to vote on the next steps in the legalization of AVS—is another way of demanding accountability.

Finally, if you work in public administrations or companies in the sector, or if you know people who do, you can **leak documents**[35] and help lift the veil on information often protected by a broadly interpreted "business confidentiality" concept.

35 To do so, you can use this secure platform: https://technopolice.fr/leak/.

B Getting organized

After the documentation stage, opposing algorithmic video surveillance requires action. It is possible to act at the national level **with institutions**. This is what La Quadrature du Net is trying to do with other associations, such as the Ligue des droits de l'Homme or Amnesty International, with some victories but limited success due to the exhaustion of democratic mechanisms and the dominance of authoritarian conceptions.

However, the most relevant and concrete action is **at the local level**, in the cities and streets where we live. Launched in 2019 by La Quadrature, the **Technopolice** initiative aims to engage a decentralized dynamic to make the different voices opposing new police surveillance technologies resonate across the territory. Since surveillance varies from city to village, we need to diversify the fronts and modes of action and adapt to local contexts and expertise.

Collectives have been set up in Marseille, Montpellier, Forcalquier, and even in Belgium! Some have succeeded in removing street microphones like in Saint-Étienne, while smaller towns have risen against the arrival of video surveillance cameras, such as Foix, Marcillac-Vallon, or Putanges-le-Lac. Collectives formed by residents are organizing everywhere to inventory, document, and fight against these technologies, while resisting the security policies imposed on them. **These local struggles are essential** to the global fight against the surveillance society and are leading to concrete victories. For example, in the PACA region, in Southern France, La Quadrature, in conjunction with local collectives, has

succeeded in banning the use of facial recognition in the region's high schools.

For these grassroots struggles, **there are many ways of taking action**. In addition to investigation, monitoring, and analysis, we can organize "mapping tours" to identify the locations and models of cameras and map them online; we can launch legal actions, write open letters to make local elected officials aware of these issues, organize information events, exhibitions, or documentary festivals around surveillance to raise awareness among residents; we can **collectively reclaim the notion of "security" and imagine emancipatory futures together**.

Finally, we need to **forge alliances**. It is essential to **articulate our struggles against police surveillance technologies with other causes**. In the Paris region, surveillance issues are part of the denunciation of the ravages caused by the Olympic Games. In Marseille, they are linked to the criticism of the gentrification that is eating away at the working-class city center and the fight against the arms industry that contributes to equipping the Israeli army. In Grenoble, they are connected to the ecological struggle against STMicro, a microprocessor manufacturing plant. There are many bridges to be built, and it is by creating solidarity between different struggles that our voices will become stronger and more powerful.

The Technopolice initiative offers a **public forum**[36] and a collaborative **documentation platform** based on the Etherpad software (known as the "Carré")[37]. Many other similar tools designed to support our struggles exist or have yet to be invented!

36 See: https://forum.technopolice.fr/.

37 See: https://carre.technopolice.fr.

C

Taking Action

The purpose of this brochure is to be distributed as widely as possible, to explain to as many people as possible the deadly political project associated with algorithmic video surveillance. This is about **taking back control**.

In the coming months, AVS experiments legalized by the Olympic Games law will be carried out throughout France. It will be **a crucial moment for mobilization**. Moreover, the text of the decree stipulates that the final assessment must take into account "the public's perception of the impact of algorithmic processing on security and the exercise of public liberties." Therefore, we must make sure that our perceptions and **our refusal of these unfair technologies** are heard.

AVS algorithms will be deployed during concerts, festivals, football matches, and Christmas markets. These events are all opportunities to express our opposition. Let's be creative! Our refusal can take the form of **a complaint letter to the CNIL**[38] or of a "suspicious" dance in front of the cameras. It could also be the opportunity to "occupy the street" to **demonstrate the surveillance** that will be deployed on people attending these events and inform them that they are the test subjects of a large-scale algorithmic analysis: **making the presence of cameras visible** by all means, handing out flyers, putting up posters[39]… there are many ways of doing this.

38 See: https://www.cnil.fr/fr/plaintes.

39 Visit our campaign page: https://laquadrature.net/vsa

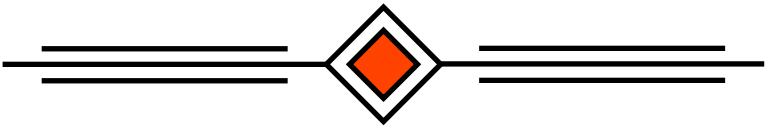
D

Taking Back Our Cities

Governments have **always been wary of cities**. That is because they have always been a place of protest. We express our anger on their walls, organize and protest in their streets. We occupy their squares and roundabouts to demand our rights. The advocates of technopolicing try to contain them with their urban security programs. After the invention of modern policing under the Ancien Régime, with the wide Haussmannian avenues that prevent barricades and large squares that favor the police, such as the Plaine, in Marseille, or the Place de la République in Paris, **AVS is now being used to muzzle us**.

In cities, we protest, but we can also leisurely stroll. We observe the architecture, draw or take pictures of it. We take care of it in our own way. We build emancipated counter-cultures, free from norms and oppression. We dance, skate, and create graffiti. We sit, party, pass the time, or explore every nook and cranny. The density of urban spaces forces us to be creative, to use the quays, squares, and benches to meet and build social relationships and solidarity, or simply do nothing. On the street, we meet strangers and experience otherness. We help repair a bike or pick up dropped groceries. We revel in the joyful chaos that cities offer us.

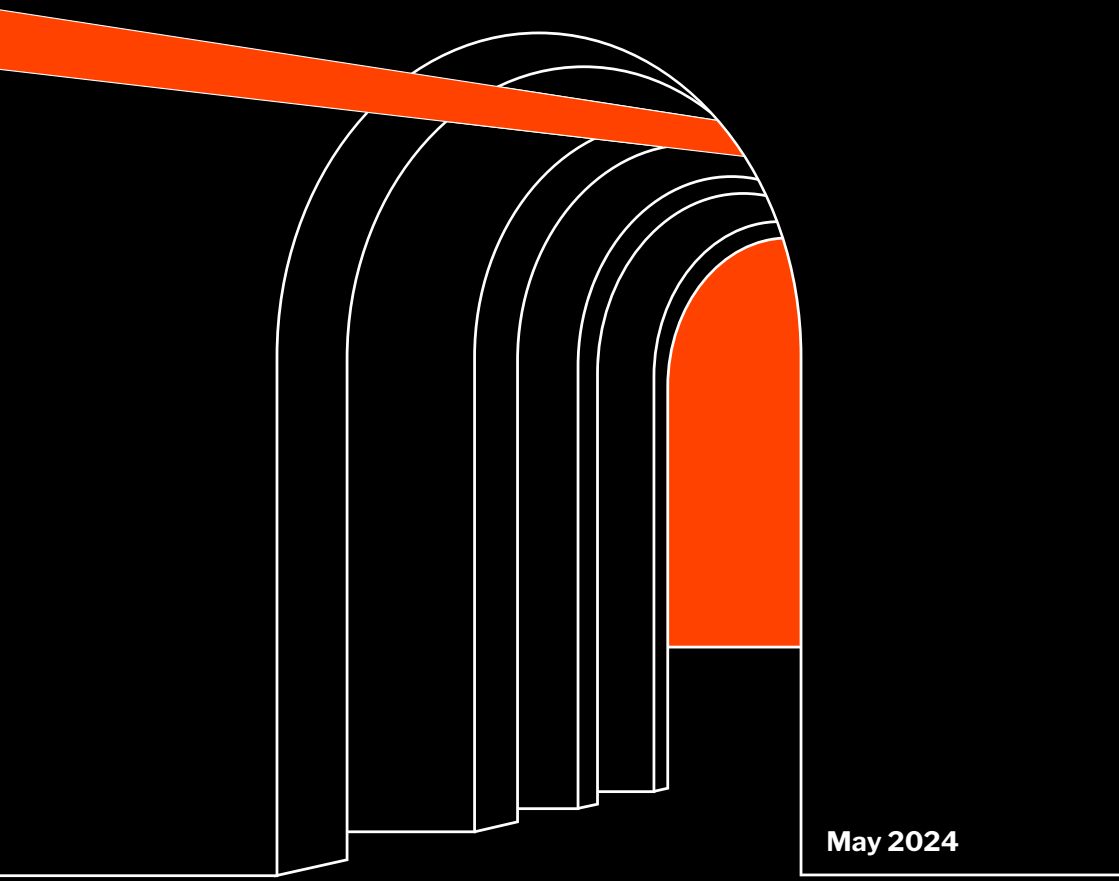
It is so that we can continue to live freely in the city that we refuse permanent, general and invisible police surveillance, that we want to keep algorithmic video surveillance and its world at bay. AVS will not pass!



Find and share

ALGORITHMIC
VIDEO SURVEILLANCE
DANGERS AND COUNTER-ATTACKS

on https://laquadrature.net/en/vsa



May 2024

La Quadrature du Net