A Panopticon for All

By Julien Le Mauff

The rise of surveillance technologies is redefining the approach to security amid economic pressures. Wherever it is implemented, this surveillance, boosted by new technologies, raises the question of abuses that threaten civil liberties.

A source of both concern and security-driven fantasy, the use of new technologies for police surveillance is no longer a remote possibility or the preserve of authoritarian regimes. Indeed, with video surveillance now widely used in public spaces across countries considered democratic, algorithmic analysis technologies are gaining ground, particularly in France, where they were officially legalized and integrated into the security apparatus for the 2024 Paris Olympic Games. Meanwhile, facial recognition has not been banned by the recently adopted the <u>EU AI Act</u>, which provides for <u>numerous exceptions</u> based on identified threats to security and order.

The deployment of innovative technologies that make extensive use of artificial intelligence constitutes both a potential market and a threat to civil liberties. The title *Technopolice* chosen by Félix Tréguer reflects the desire to take both of these factors into account in an essay that is the result of a journey combining research and activism.

An ideal of permanent control

Already the author of <u>Contre-histoire d'Internet</u> (Fayard, 2019, reprinted by Agone, 2023), Tréguer has expanded his research as a member of the association La Quadrature du Net. For the past 15 years, this association has been an <u>active advocate</u> for issues related to the protection of personal data and online freedoms. Drawing on this experience, the ideas presented in *Technopolice* give way to personal accounts, accompanied by insightful theoretical reflections. The result is a blend of journalistic investigation and in-depth analysis of the discourse and struggles surrounding police technology.

Tracing the development of the concept of "technopolicing", the author recalls its almost simultaneous emergence, not only <u>in a critical manner by an initiative that brings together some 30 associations</u>[1], but also in a much more programmatic way, as the title of a series of "technical and operational days on internal security" organized by the French Ministry of the Interior. These events, which are attended by government departments and representatives of large private companies and start-ups, show that "facial recognition is already widely integrated into police practices" (p. 27) — a finding that recent evidence has shown is accompanied by <u>uses that are both very specific and completely illegal</u>.

As summarized in a note issued by the Research Center of the National Gendarmerie Officers' Academy (CREOGN) cited by the author[2], on the "issue of acceptability" of facial recognition, the advantage of this technology would be to make "identity checks *permanent* and *universal*" (p. 32), a modern version of Foucault's panopticon that would apply to everyone everywhere, eliminating any possibility of anonymity: "moving about with your face uncovered would be like carrying a forgery-proof ID card that could be read at any time" (p. 36).

---

[1] These included not only La Quadrature du net, <u>but also the Ligue des droits de l'homme (Human Rights League) and the Syndicat de la magistrature (Magistrates' Union)</u>.

[2] Dominique Schoenhoer, <u>*Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité*</u>, CREOGN note, n° 43, 2019.

"Safe City" and "datapolice"

The author also looks at the rise in techno-security discourse, which is particularly evident in projects involving local authorities (as seen in the cities of Nice, Dijon, Marseille, etc.) and industrial groups. These projects, known as "Safe City," add a security component to the concept of the connected "smart" city. However, such constructions are part of a technocratic project aimed at "shielding neoliberal capitalism from the social and ecological crises that it continues to generate" (p. 64). For this reason, the Safe City project "can be interpreted as a *mechanism of power*": the argument thus effectively extends the Foucauldian reference — albeit expected — to *Discipline and Punish* (1975), in which the philosopher described the modern shift from a punitive society to "panopticism," ensuring individual discipline through the guarantee of perpetual surveillance.

In light of this, it seems there is no way to resist projects that involve so many actors, have the government's backing, and lead local politicians — even those who have spoken out against the expansion of video surveillance — to ultimately integrate the innovative tools of the "Safe City" into a true "continuum between urban and police management" (p. 91). However, this is only the latest stage in a long process of reframing social issues in terms of security, which the author shows has been part of political decision-making since the 1990s, particularly in France within the Socialist Party. As well as turning popular expressions of anger or revolt into behavioral problems that can be punished, this change especially affects "undesirables", such as a young Roma woman arrested for shoplifting and subject to a deportation order after facial recognition software identified her as having a "69% similarity" to a person who did not resemble her but was subject to an order to leave the country.

The article goes on to show how the logic of rationalizing police work through technology is also imposed on police officers themselves; furthermore, while failing to prevent abuses in a situation that will always be asymmetrical for users, it places their actions and behavior under pressure from new obligations aimed at expanding databases, and from a policy of numbers, all of which largely transform police work into a data management task and contribute to the dehumanization of the police's relationship with the public (pp. 101-140).

Furthering the cause of security

Alongside the disturbing list of rights violations, biases, and abuses in the use of new police technologies, the investigation also highlights the mobilization of private interests and political entrepreneurs in a full-fledged battle to control the narrative. For these actors, the challenge is to promote a pro-technology vision that identifies the development of security technologies as an economic opportunity. In this vast market, national groups should be supported as they face competition from foreign companies, particularly from China and Israel. Furthermore, aside from the belief put forward by these actors that "biometrics is inevitable" (p. 29), or that "the added value of [facial recognition] for the police is beyond doubt" (p. 32), the association of public and private actors forming an "*interstitial* field" with blurred boundaries (p. 145), and within common structures, seems to be aimed at aligning public resources (and public procurement) with industrial ends.

This occurs, in particular, through a capture (pp. 37-47) of numerous sources of public research funding, both in the form of direct European (Horizon Europe, ERDF) and national (Bpifrance) grants and through tax breaks (research tax credit in France). But this industrial strategy, which regards "technopolicing" primarily as an economic opportunity, is also reflected in pressure to relax plans to ban facial recognition in European legislation (pp. 165–182) and, above all, in the introduction of exceptions that are no longer justified solely by urgent public order requirements, but also by the need to foster innovation. These "sandboxes"—which are exempt from personal data laws under the pretext of technological experimentation—are an extension of a "small steps" strategy that, for several decades, has led to countless examples of exceptional measures being incorporated into common law and used for repressive purposes that are much less isolated than initially promised. The developments that enabled algorithmic video surveillance in public spaces to be implemented during the 2024 Paris Olympics are a textbook case, with the French government having already announced its desire to make it a permanent tool.

Similarly, the equivocal role of France's National Commission on Informatics and Liberties (CNIL), which the author highlights on several occasions, shows how this body has shifted from being a regulator and supervisor of practices to a compliance tool, helping private actors to bring their actions into line with regulations rather than restricting them through repressive measures. Anne Bellon, whom Tréguer cites, has noted how changes in personal data legislation, particularly under the

influence of the personal data processing requirements created by the European GDPR, "have led to the emergence of a new compliance market," and how the CNIL is fully involved in this[3], which National Assembly member Philippe Latombe — a fervent supporter of video surveillance — sums up by stating that "the CNIL has opened its chakras" and now "integrates social, technological, and economic realities" (p. 163).

A totalitarian agenda?

The technopolicing issue is a particularly striking illustration of how the state seems to be relinquishing its role as guarantor of civil rights and liberties at a time when the balance of power is being reconfigured. It may seem somewhat paradoxical to conclude the essay by stating that "the technopolice is tending towards *totalitarianism*" (p. 183). For while Abraham Bosse's frontispiece for Thomas Hobbes's *Leviathan* (1651) is worth revisiting from the perspective of police surveillance (pp. 67-68), the developments that quite directly "derive" technopolicing from state policy (pp. 63–73) do not explain this apparent contradiction between the weakening of state sovereignty and the expansion of police surveillance capabilities. To this end, we could explore the key reference to Carl Schmitt (p. 174) in greater depth and place it within the long evolution of emergency policies, so as to better understand the advent of a new paradigm, one that opposes a "quantitative" total state extending its areas of intervention to the social sphere, and promotes a state that is "total in terms of quality and energy" and focused on maintaining order in the service of private interests and "authoritarian liberalism"[4].

For, as Félix Tréguer points out (p. 173), these concessions and the French government's rhetoric of the "Start-up nation" illustrate the "trading of legal sovereignty"[5] noted by Benjamin Lemoine and Antoine Vauchez. As a result, the power to regulate and establish the law is being redistributed, not simply as a result of pressure from private actors, but of, on the one hand, a "counterculture of

---

[3] Anne Bellon, « Protéger les données. Entre mission politique et pratiques administratives, enquête sur le travail de la CNIL », in Anaïs Theviot (ed.), *Gouverner par les données ? Pour une sociologie politique du numérique*, Paris, ENS Éd., pp. 71-92.

[4] Carl Schmitt, Hermann Heller, *Du libéralisme autoritaire*, translated and presented by Grégoire Chamayou, Paris, Zones, 2020.

[5] Benjamin Lemoine and Antoine Vauchez (ed.), « Affaires publiques, intérêts privés », special issue of *Actes de la recherche en sciences sociales*, n° 251, 2024.

government" that is transforming the state into an agent of its own deregulation, and, on the other hand, its neoliberal transformation into a <u>multiplicity of public authorities with more limited mandates</u>.[6] The rise of surveillance tech can be seen as one sign of a broader problem: an anti-democratic "authoritarian spiral," which is even more threatening because of the unprecedented control offered by technopolicing.

---

[6] See also Antoine Vauchez, *Le Moment régulateur. Naissance d'une contre-culture de gouvernement*, Paris, Presses de Sciences Po, 2024.