Big Brother is Watching the Olympic Games - and Everything Else in Public Spaces

Sophie Duroy

22.03.2023 doi: 10.17176/20230322-185302-0

The French National Assembly is currently debating the law on the 2024 Olympic and Paralympic Games. Despite its name, the law has more to do with security than sports. In particular, Article 7 of the law creates a legal basis for algorithmic video surveillance, that is, video surveillance that relies on artificial intelligence to treat the images and audio of video surveillance cameras in order to identify human beings, objects, or specific situations. In other words, video surveillance cameras in France's public spaces would now be able to identify you and detect if your behaviour is suspicious. Admittedly, this is already the case in several French cities (for instance in Toulouse since 2016) and in some railway services, but without any legal basis.

France is infamous for its attachment to surveillance, with the highest administrative court even deciding to ignore a CJEU's ruling concerning its mass surveillance measures on the ground that the protection of national security is part of the "national identity" of the country. However, Article 7 represents a major step in the direction of general biometric mass surveillance and should be of concern to everyone. In fact, the risks posed by AVS are so high that the current discussions on the European Regulation on Artificial Intelligence envision a formal ban.

The legal basis for AVS provided by Article 7 of the new French law is especially worrisome from two perspectives. First, it would legitimise a practice that is in violation of France's human rights obligations. Second, adopting this law would make France the first EU member state to grant a legal basis to algorithmic video surveillance (AVS), thus creating a worrisome precedent and normalising biometric mass surveillance.

Background

The French government already unsuccessfully tried to include the authorisation of AVS in its 2021 law on 'Global Security' and in a more recent programmatic law concerning the ministry of interior (LOPMI). The bill on the Olympic and Paralympic Games was introduced in Parliament by the French government on 22 December 2022 and subjected to an accelerated procedure. It was adopted by the French Senate on 31 January 2023, and brought before the National Assembly on 10 February 2023. Following a commission reading and amendments, a plenary debate and vote began on 20 March 2023.

The current political and social tensions regarding the pension reform, forced through Parliament in the same timeline, have left little visibility to this other bill. Nevertheless, both La Quadrature du Net and an open letter signed by 38 European civil society organisations have attempted to raise attention to the bill in order to mobilise support against Article 7.

On paper, Article 7 appears more innocuous than it really is. Indeed, its first paragraph clearly states that AVS is to be used only for purposes of experimentation, until 31 December 2024 (originally 30 June 2025), and that its sole aim is to "ensure the security of sporting, recreational or cultural events which, because of the scale of their attendance or the circumstances in which they take place, are particularly exposed to the risk of acts of terrorism or serious threats to the safety of individuals". It also explicitly states that the algorithmic processing of data "shall not use any biometric identification system, process any biometric data or implement any facial recognition technique". I will come back to these two points throughout the blog, looking first at the purpose and

aim of AVS in light of France's human rights obligations, and then at the effect of the bill with regard to the normalisation of biometric mass surveillance.

Article 7 and France's Human Rights Obligations

AVS clearly constitutes an infringement on the right to privacy and on freedom of assembly and association. It also has a chilling effect on many human rights. As highlighted by the former UN Special Rapporteur on Counterterrorism and Human Rights, privacy also serves as a basis for other rights, meaning that freedom of expression, association, and movement all require privacy to be able to develop effectively. Knowing that one is constantly subjected to algorithmic-driven surveillance necessarily leads to inhibitions due to (legitimate) fears of being identified, profiled, discriminated against, and possibly wrongfully prosecuted. Indeed, surveillance measures regularly lead to wrongful arrests, failures of due process and miscarriages of justice, therefore affecting the rights to liberty and security of the person, to a fair trial, and to be afforded due process. Finally, the biases embedded in algorithmic-driven mass surveillance are serious and have been evidenced in many contexts, including counterterrorism. Its use may thus also be in breach of the right to non-discrimination.

When it comes to the right to privacy and freedom of assembly an association, human rights courts and bodies have established a four-part proportionality test that must be passed for restrictions to these rights to be lawful. The restriction must be in accordance with law; pursue a legitimate aim; be necessary; and be proportionate in the strict sense.

Article 7 would undoubtedly provide a legal basis for the use of AVS (in contrast with its current use in France that is devoid of any legal basis and, as such, is clearly unlawful under international human rights law). The aim pursued will likely be recognised as a legitimate one, since the protection of national security and public order figure in the listed aims able to justify restrictions to the rights at stake. The issues therefore lie further ahead, with necessity and proportionality.

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure with regard to the aim pursued and of whether it is less intrusive compared to other options for achieving the same goal. Relatedly, proportionality in the strict sense requires that the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of the fundamental rights.

It bears emphasising here that the burden of proof is on the government. In other words, the government must demonstrate, using appropriate data and evidence, that AVS is both effective and the least intrusive measure to effectively secure national security and public order. Furthermore, the government will need to show that the restrictions upon the right to privacy and freedom of assembly and association are outweighed by the benefits of AVS. Such justifications are currently missing from both the law and the public discourse surrounding it. Ironically, they are also missing from research. The effectiveness of video surveillance to counter national security threats has never been demonstrated and, with regard to common crimes, it is more than doubtful.

Further, terrorism's extremely low base rate means that false positives are the norm. In fact, using facial recognition software would lead to the correct identification of a terrorist in less than one case out of a thousand, meaning that 99,91% of the terrorists identified by facial recognition are actually not terrorists at all (Schulan, Table 2). Since AVS and facial recognition are based on the same image analysis and biometric surveillance algorithms (the former isolates and recognises bodies, movements or objects, while the latter detects a face), this finding is particularly concerning.

In the context of France's use of AVS, the algorithm will identify people as 'suspicious' based on what humans have taught it are behaviours or physiological features associated with national security threats. However, because these national security threats are so rare, the algorithm will flag, for the vast majority, individuals who are not posing any threat. The discriminatory aspects of the measure are obvious.

People belonging to racial, ethnic, and religious minorities and marginalised people (for instance, standing immobile for more than 300 seconds – a common behaviour for homeless people – is considered suspicious) are the most likely to be flagged as risky, meaning they will be overly targeted, policed, and stigmatised as a result. Deep learning will then only perpetuate the biases and fallacies embedded in the original algorithm.

Moreover, as emphasised by the open letter, there is a strong case to be made that AVS threatens the very essence of the right to privacy and data protection, hence rendering the proportionality analysis unnecessary.

Normalising Biometric Mass Surveillance

Despite the statement contained in the law that AVS will not "use any biometric identification system, process any biometric data or implement any facial recognition technique", its very functioning implies the collection and processing of biometric data. Biometric data is defined in the General Data Protection Regulation (GDPR, Art. 14) as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person". As emphasised by the open letter, it would be impossible to detect suspicious events in public space without collecting and processing the physical, physiological and behavioural features of the individuals present in the public space. The effectiveness of the system further rests on the possibility to isolate individuals in a crowd, thereby leading to their "unique identification" – regardless of whether their name or ID number is known. Hence, Article 7 constitutes an effective legalisation of biometric mass surveillance.

In addition, while the use of AVS is presented as an experiment in the law, experience and research clearly show the strong lock-in and mission creep effects of national security measures. The French experience in this regard is enlightening. The proclamation of a state of emergency on the night of the attacks of 13 November 2015 was followed by six prolongations, leading the state of emergency to last until 1 November 2017 – just short of two years. However, this termination was only made possible because most of its measures were, in the meantime, codified into ordinary law, so as to apply outside any declared state of emergency. France's struggles to exit the state of emergency, and its exit mostly in name, illustrate well how the fear of future threats to national security justifies the continued strengthening of national security measures, ultimately rendering governments incapable of restoring the rights and freedoms they have sacrificed in its name.

Furthermore, both the Council of State and the Constitutional Council found it lawful and constitutional, respectively, to apply the administrative measures (in particular house arrest) authorised by the state of emergency, proclaimed due to the risk of terrorist attacks from the Islamic State, to climate activists during COP21 in December 2015. In other words, the declared purpose and aim of national security measures do not bind the government. When a measure is considered lawful, it can be lawfully used beyond the original objective justifying its authorisation. Hence, the fact that AVS is presented as necessary to secure the Olympic and Paralympic Games (as well as other events of a similar scale) should not constitute a guarantee that it will not be used outside this scope. On the contrary, experience shows that the most likely scenario is that of AVS being used to identify all types of criminal behaviour, in all public spaces. France would, in this regard, join other states that have used sporting events to test and make acceptable surveillance technologies. These include Russia, China, and Qatar.

Conclusion

With the law being currently debated in Parliament and the possibility of a Constitutional Council review before promulgation, it is still too early to know whether France will join Russia, China, and Qatar in using sporting events to boost its surveillance apparatus. However, it is not a coincidence that the French government, after two unsuccessful attempts, is now using a bill on the Olympic and Paralympic Games as a

pretext to authorise AVS. The scale and demands of the Olympics, like states of emergency, allow for the normalisation of the exceptional. In other words, "it is not surveillance technologies that serve the Olympics, but the opposite. They entail the opportunity to advance a political and economic agenda that requires surveillance mechanisms to be as effective, widespread and accepted as possible" (Viegas Ferrari p. 92). What remains to be seen is whether France's attachment to its surveillance capabilities is higher than its commitment to European rule of law and fundamental rights values.

ABOUT THE AUTHOR

Sophie Duroy
Dr. Sophie Duroy is a Lecturer at Essex Law School and Human Rights Centre, University of Essex.Dr. Sophie Duroy is a Lecturer at Essex Law School and Human Rights Centre, University of Essex.

SUGGESTED CITATION

Duroy, Sophie: Big Brother is Watching the Olympic Games – and Everything Else in Public Spaces, Verfassungsblog, 22.03.2023, doi: 10.17176/20230322-185302-0.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20230322-185302-0.