Civil society public letter
on the proposed French law
on the 2024 Olympic and Paralympic Games

Dear Members of Assemblée nationale,

We, the undersigned **38 civil society organisations**, are writing to **express our deep concern regarding Article 7** of the proposed law on the 2024 Olympic and Paralympic Games (*projet de loi relatif aux jeux Olympiques et Paralympiques de 2024*[1]*)*. This provision creates a legal basis for the use of algorithm-driven cameras to detect specific suspicious events in public spaces.

The proposal paves the way for the use of **invasive algorithm-driven video surveillance** under the pretext of securing big events. Under this law, France would become the first EU member state to explicitly legalise such practices. We believe that the proposed surveillance measures **violate international human rights law** as they contravene the principles of necessity and proportionality, and pose unacceptable risks to fundamental rights, such as the right to privacy, the freedom of assembly and association, and the right to non-discrimination.

We call on you to consider rejecting Article 7 and to open up the issue for further discussion with civil society. Otherwise, its adoption would establish a worrying precedent of unjustified and disproportionate surveillance in publicly accessible spaces to the detriment to fundamental rights and freedoms.

The proposal constitutes a serious threat to civic freedoms and democratic principles

The mere existence of untargeted (often called indiscriminate) algorithmic video surveillance in publicly accessible areas can have **a chilling effect on fundamental civic freedoms**, especially the right to freedom of assembly, association and expression. As noted by the European Data Protection Board and the European Data Protection Supervisor,[2] biometric surveillance stifles people's reasonable expectation of anonymity in public spaces and reduces their will and ability to exercise their civic freedoms, for fear of being identified, profiled or even wrongly

[1] https://www.senat.fr/leg/pjl22-220.html

[2] https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf

prosecuted. As such, this measure **threatens the very essence of the right to privacy and data protection**, which is incompatible with international and European human rights law.

In line with democratic values and principles, upholding the full protection of these fundamental rights and creating enabling conditions for public debate, including political expression in public spaces, is especially crucial during important events, such as the Olympics.

What is more, the proposed legislation significantly and dangerously expands the reasons justifying the surveillance of public spaces. The classification of situations such as begging or stationary assemblies as "atypical" creates **the risk of stigmatisation and discrimination** of people who spend more time in public spaces, for example due to their homelessness, economic vulnerabilities or disability. Evidence has shown that the use of surveillance technologies creates a state of permanent monitoring, profiling, and tracking that disproportionately harms marginalised people. Using algorithmic systems to fight crime has resulted in over-policing, structural discrimination in the criminal justice system, and over-criminalization of racial, ethnic and religious minorities, leading to the violation, among others, of the principle of non-discrimination enshrined in international and European human rights standards.

The proposal would lead to biometric mass surveillance

Article 7 - III of the proposed law wrongly asserts that algorithmic video surveillance systems will not process biometric data. The EU General Data Protection Regulation (GDPR) defines biometric data 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"* (Article 4(14) of the GDPR). If the purpose of algorithm-driven cameras is to detect specific suspicious events in public spaces, **they will necessarily capture and analyse physiological features and behaviours of individuals present in these spaces**, such as their body positions, gait, movements, gestures, or appearance. Isolating individuals from the background, without which it would be impossible to achieve the aim of the system, will amount to "unique identification". As established by EU data protection law, and as interpreted by the European Data Protection Board[3], the ability to single a person out from a crowd or their surroundings, regardless of whether the person's name or ID number is known, constitutes "unique identification".

[3] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

It is important to remember that the use of AI-based systems to analyse and predict people's behaviours, emotions or intentions can be equally as invasive and dangerous as those which are used to identify people. Classifying people as exhibiting “risky” behaviour based on their biometric data **would amount to biometric categorisation**, defined by the French Défenseur des droits and the proposed EU Artificial Intelligence Act as assigning natural persons to specific categories based on their biometric features. We bring to your attention that this measure risks colliding with the future EU AI Act. While legislative work is still ongoing, a number of parliamentary amendments propose to prohibit biometric categorisation entirely, given their severe risks to fundamental rights.

The serious interference with human rights does not meet the requirements of necessity and proportionality

Effective human rights protection begins with understanding the limits of technologies and presenting evidence that they are indeed fit for purpose. A corollary of that is the need to investigate how technologies introduced in the name of security respond to actual threats and how they will impact human rights and civic freedoms.

Despite this proposed law presenting a grave risk to fundamental human rights and existing evidence[4] of actual inefficiency of video surveillance to prevent crime or security threats, the government **has not demonstrated how this proposal meets the principles of necessity and proportionality**, nor meaningfully engaged with civil society about the measure. As such, we believe that the proposed restrictions to human rights do not meet the three-part test of legality, legitimate aim, and necessity and proportionality. This is a violation of the state’s human rights obligations, imposed by international treaties, such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

The proposal is a step towards the normalisation of exceptional surveillance powers

The proposed Article 7 is indicative of a worrying trend of governments expanding their surveillance powers as an emergency measure in the name of security. Yet rarely are these “exceptional” measures promptly revoked. Instead, **surveillance and control become normalised**, often lacking appropriate safeguards, transparency, stakeholder engagement and accountability mechanisms.

This has notably been the case for surveillance measures introduced over the last 20 years in the name of counterterrorism and more recently – with digital

[4] https://www.lemonde.fr/societe/article/2021/12/22/une-etude-commandee-par-les-gendarmes-montre-la-relative-inefficacite-de-la-videosurveillance_6106952_3224.html

solutions adopted during the Covid-19 pandemic[5]. But we have also seen that **previous Olympic games similarly served as a terrain for experimentation**[6] with increased state powers later repurposed for non-emergency situations.

These experiences provide valid justification for our concern that algorithmic video surveillance will not be abandoned after 2025. If adopted, this law will also set a **dangerous precedent for other European countries** which have - so far unsuccessfully - attempted to legalise a range of risky biometric surveillance practices, including Portugal and Serbia. France would then become an infamous "leader" in surveillance policies within the European Union.

We sincerely hope that you will take urgent steps in consultation with civil society to address the concerns outlined in this letter. We remain available to further elaborate on the issues raised.

Yours sincerely,

Access Now, Global
AlgoRace, Spain
AlgorithmWatch, Germany
AlgorithmWatch CH, Switzerland
Amnesty International, Global
ApTI, Romania
ARTICLE 19, Global
Association Nationale des Supporters, France
Big Brother Watch, UK
Bits of Freedom, The Netherlands
Centre for Democracy & Technology, Europe
Chaos Computer Club Lëtzebuerg, Luxembourg
Citizen D / Državljan D, Slovenia
Civil Liberties Union for Europe, Europe
Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany
Digitalcourage e.V., Germany
Digitale Gesellschaft, Switzerland
Digitale Freiheit e.V., Germany
Elektronisk Forpost Norge, Norway
Eticas Tech, Spain
European Center for Not-for-Profit Law Stichting (ECNL), Europe
European Digital Rights, Europe
Fair Trials, Global

[5] https://ecnl.org/publications/under-surveillance-misuse-technologies-emergency-responses

[6] https://www.scielo.br/j/cm/a/zcKnN9ChT9Wqc4hfGWKSk4d/?format=pdf&lang=en

Forum Civique Européen, France/Europe
Football Supporters Europe, Europe
Homo Digitalis, Greece
Human Rights Watch, International
Irish Council for Civil Liberties, Ireland
IT-Pol, Denmark
Iuridicum Remedium, Czech Republic
Liberty, UK
Panoptykon Foundation, Poland
Privacy International, Global
Privacy Network, Italy
Share Foundation, Serbia
Society Vrijbit, The Netherlands
Statewatch, Europe
Today is a new day / Danes je nov dan, Slovenia