



Manchester
Metropolitan
University

AI-DRIVEN MASS SURVEILLANCE AT 2024 OLYMPICS: THE HUMAN RIGHTS ISSUES AND RECOMMENDATIONS

Dr Aikaterini Koula

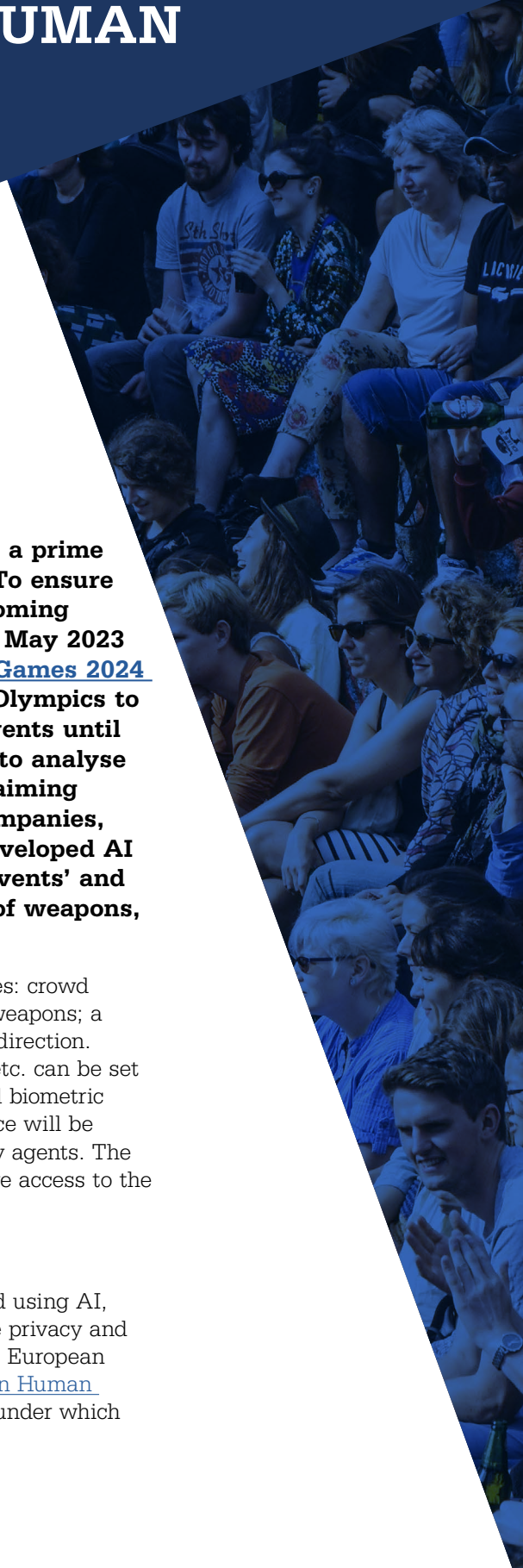
Brief Overview of the Situation

The Olympics are a major world event and therefore they are a prime target for terrorists who hope to stage a high-profile attack. To ensure the protection of the public, the smooth operation of the upcoming Olympic Games, and the prevention of terrorist acts, on 19th May 2023 the French government passed the [Olympic and Paralympic Games 2024 Act](#). This allows the use of AI video surveillance during the Olympics to detect abnormal events or human behaviour at large-scale events until late June 2025. AI-powered surveillance employs algorithms to analyse real-time video streams from existing surveillance systems, aiming to identify potential threats in public spaces. Four French companies, Videtics, Orange Business, ChapsVision and Wintics, have developed AI software for this purpose, trained to detect predetermined 'events' and 'abnormal' behaviour, such as crowd surges or the presence of weapons, and send alerts to human operators for evaluation.

The law permits the identification of eight specific events during the Games: crowd surges; abnormally heavy crowds; abandoned objects; presence or use of weapons; a person on the ground; a fire breaking out; contravention of rules on traffic direction. Certain thresholds, such as the number of people, type of vehicle, timing etc. can be set manually for each event, location or threat. However, facial recognition and biometric identification remain banned under the French law. AI-powered surveillance will be used by national and local police, firefighters, and public transport security agents. The latter will operate under the authority of the Police Prefecture who will have access to the premises where these security agents conduct their services.

Wider Legal Context

A wider spectrum of rights needs to be considered when developing or/and using AI, depending on the technology and its area of application. Key rights include privacy and data protection, equality and non-discrimination, and access to justice. All European Union (EU) Member States are state Parties to the [European Convention on Human Rights](#) (ECHR) which outlines these rights and establishes the conditions under which interference(s) with human rights and freedoms may be justified.



The [Charter of Fundamental Rights of the European Union](#) (CFREU) is the EU's Bill of Rights and includes all ECHR rights. In addition to ECHR provisions, the Charter addresses some more modern aspects, such as human cloning.

On 13th March 2024, the EU adopted the [The European Union Artificial Intelligence \(AI\) Act](#) (thereafter EU AIA) which is a legally binding instrument on all 27 Member States, including France, and addresses the risks of AI.

The EU AIA is a cross-sector regulation applicable to all public and private organisations developing or/ and using AI in the EU. It establishes a risk-based approach, categorising AI systems based on their potential to harm individuals' fundamental rights and society as a whole into four categories: unacceptable risk, high-risk, limited risk, and minimal risk. The EU AIA completely bans a limited number of AI applications due to the unacceptable risk they pose, such as the exploitation of vulnerabilities and biometric categorisation. According to EU AIA, the real-time use of facial recognition by law enforcement is prohibited in principle, except in exhaustively listed and narrowly defined situations. Such situations may include, for instance, preventing a terrorist attack.

Although AI can enhance security during the Games, algorithmic surveillance can lead to false positives, the amplification of potential biases, privacy infringements and violations of fundamental human rights.

The Human Rights Issues

- **Widespread Tracking and Monitoring:**

The extensive tracking and monitoring of millions of individuals represent a pervasive intrusion into their privacy. Under Article 8 of the ECHR, all individuals have the right to private life, which includes the protection of their privacy and data. Similarly, Article 8 of the EU Charter specifies data protection as an integral aspect of private life. Interferences with this right may be possible only to protect legitimate aims, such as national security or public order, but they must always be proportionate to the aim pursued. AI algorithms continuously scan and collect data from individuals within their range, potentially capturing sensitive personal information without consent (e.g., smoking habits, sexual orientation). Although the European Court of Human Rights (ECtHR) has not yet ruled on the use of AI, it has emphasised the need for clear safeguards against mass surveillance and the implications for the right to privacy in cases such as *Big Brother Watch v. United Kingdom* and *Roman Zakharov v. Russia*.

- **Broad Definitions of Suspicious Activity:**

Officials' broad definitions of 'suspicious' and 'abnormal' activities raise concerns about subjective categorisations that could infringe on individuals' privacy and liberty rights (e.g., arrests and short detention) and lead to the cancellation of sporting and cultural events. Under Article 5 of the ECHR, no one should be deprived of their liberty except under specific circumstances, such as lawful

detention following conviction by a competent court, or arrest or detention due to noncompliance with a lawful court order. Broad applications of terms like 'suspicious' and 'abnormal' could result in the deprivation of liberty for individuals whose activities are not genuinely suspicious or abnormal, thereby breaching Article 5.

- **False positives:** Algorithms may produce false positive results that even a human operator is unable to distinguish, particularly when the reliance on AI models for accuracy is high. This failure to identify true positives could lead to a series of human rights infringements for individuals (e.g., arrest, detention) and the broader community (e.g., cancellation of events, road closures).
- **Freedom of Expression and Assembly:** The omnipresence of AI-driven surveillance mechanisms at the Games creates an environment where individuals may feel constantly observed by technologies that many may not fully understand. This constant surveillance can have a chilling effect on individuals' behaviour, as they may alter their actions, or avoid interacting with certain people to prevent being flagged as suspicious. Moreover, as a consequence of surveillance, national authorities may postpone or cancel protests or events, undermining the rights of expression and assembly. Under Articles 10 and 11 ECHR, individuals are entitled to the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities. They also have the right to peaceful assembly and association. As stated above, interferences with these rights may be justifiable, but they must pursue legitimate aims and be proportionate to those aims. The implementation of the French Law could lead to an overreliance on surveillance to justify the cancellation of protests or events without well-founded reasons, and risks infringing upon these fundamental freedoms.
- **Potential Discriminatory Impacts:** The surveillance measures may disproportionately affect certain communities, such as communities of colour and migrants or ethnic minorities. The reason is that discrimination may also occur at the stage of data processing and at the machine learning stage, potentially leading to biased outcomes that perpetuate discrimination against minorities and marginalised communities. For instance, data analysis might show that a specific minority group, [let's call them] X, has been linked to most terrorist attacks in France. Consequently, algorithms could be trained to associate individuals from group X with a higher likelihood of involvement in terrorist activities. This process may result in the creation of 'risk profiles' that indirectly discriminate based on race or ethnicity. In turn, these groups could be subject to heightened scrutiny and surveillance, leading to further marginalisation and discrimination. Such practices are prohibited under Article 14 of the ECHR, which ensures that all individuals enjoy their rights and freedoms without discrimination on any ground, including race, colour, language, or national

or social origin. In essence, these discriminatory practices can infringe on other fundamental human rights, such as the right to privacy, liberty, and freedom of association and assembly.

- **Risk of Data Misuse:** The vast amount of data collected through surveillance creates a risk of misuse or abuse. There is therefore potential for the misuse of personal data, such as profiling individuals based on their behaviour or targeting specific groups for discriminatory purposes, violating Article 14 of the ECHR.

Recommendations

In advance of the upcoming 2024 Olympic Games in Paris, and for future Olympic editions where AI technology may be used, the following recommendations are proposed. These are to ensure better human rights compliance by the French authorities, and associated private operators, ensuring the full respect, protection, and fulfilment of the rights of all individuals attending the Paris Games.

- The cameras should be exclusively deployed during sporting, recreational, or cultural events that are deemed high-risk targets for potential terrorist attacks, after an adequate risk assessment has been carried out by the relevant authorities.
- The use of biometric identification and facial recognition should occur only within narrowly defined situations and provided that less intrusive measures would not be effective. Such data should not be stored, as they can directly identify individuals.
- State authorities responsible for implementing AI surveillance systems should undergo thorough trainings on the classification of 'suspicious' and 'abnormal' activity. This training is crucial to ensure objective and consistent practices and to address potential biases in handling such data.
- Any interference with the rights of expression and assembly, such as the cancellation of protests or the postponement of events, as a result of the use of surveillance mechanisms, should meet the requirements of necessity and proportionality. This means that any action taken must be absolutely necessary to ensure public safety, without any less intrusive alternatives available. The rationale behind such measures should be publicly disclosed for transparency.
- Software companies should adhere to all statistical and data science methodologies and processes to ensure that all models used to train the algorithms are balanced and unbiased. All prohibited grounds of discrimination as listed in the ECHR and EU Charter are relevant in both the training and use of algorithms.

- Public authorities should ensure that everyone involved in data processing complies with French and European data protection legislation as well as the ECHR.
- Public authorities should transparently identify the entity responsible for processing personal data, specify the events subject to monitoring, and clarify the reasons, locations, and duration of surveillance. Any individual decisions to implement the system should be subject to legal challenge in court to uphold accountability.
- Following past Olympics, several surveillance measures initially implemented for the events became permanent, such as the deployment of extensive CCTV systems in host cities, such as the UK (2012) and Athens (2004). Despite the time-limited status of the legislation, the French government should ensure that the law will not be extended and provide safeguards to prevent the establishment of a permanent surveillance infrastructure.

References

- Article 10, [Olympic and Paralympic Games 2024 Act](#) (in French)
- Constitutional Court of France. [Decision on Surveillance 2023-850 DC](#) (in French)
- [The European Union AI Act](#), 13 March 2024.
- [European Convention on Human Rights](#) (1950).
- [The Charter of Fundamental Rights of the European Union](#) (2000).
- [Big Brother Watch and others v. United Kingdom](#) (2021).
- [Roman Zakharov v. Russia](#) (2015).
- European Union Agency for Fundamental Rights ['Bias in Algorithms: Artificial Intelligence and Discrimination'](#) (2022).

Further Information

Dr Aikaterini Koula is a Lecturer in Law at Manchester Metropolitan Law School and her research lies within International Human Rights Law with focus on the legal aspects of the activities of Human Rights Defenders as well as the human rights violations against them.

Contact:

A.Koula@mmu.ac.uk