Utrecht University

FACIAL RECOGNITION TECHNOLOGIES AND ALGORITHMIC VIDEO TECHNOLOGIES FOR MASS SURVEILLANCE IN TERMS OF THE RIGHT TO PRIVACY: A CASE STUDY OF PARIS OLYMPIC GAMES 2024

STUDENT: LAURA CATALINA GARZÓN VALENZUELA
STUDENT ID: 8789231

SUPERVISOR: DR. EVELIEN BROUWER

SECOND READER: DR. LISETTE MUSTERT

JULY 5TH, 2024

Table of Contents

INTRODUCTION

I. Background

Since before the digitalization of society, the state power of surveillance has been controversial. On the one hand, governments have used surveillance as a tool for control of the masses since it concerns a (under certain circumstances) necessary and legitimate power to control people to prevent risks for the public order, health or national security.[1] A clear example is the possibility of surveillance for investigative purposes in cases where a person is suspected to be committing criminal offenses, as for example wiretapping.[2] On the other hand, government control, at least in democratic states, has its limits within the recognition of fundamental rights. An example of this limitation is the negative obligation that states must abstain from interfering with the right to private and family life.[3]

AI systems are machine-based systems designed to operate with varying levels of autonomy, which may exhibit adaptiveness after deployment and that, for specific purposes, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[4] Now, facial recognition technologies, commonly referred to as FRTs, represent a distinct subset within the realm of biometric technologies. They encompass a broad spectrum of applications, extending from basic facial detection in visual data to the sophisticated processes of verification, identification, and the categorization or classification of individuals.[5] FRTs revolve around managing biometric data, understood 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, such as facial images or

[1] See Jennifer A Brobst, 'The Metal Eye: Ethical Regulation of the State's Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement' (2018) 55 California Western Law Review 1, 12.
[2] See 'House of Lords - Surveillance: Citizens and the State - Constitution Committee' <https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm> accessed 28 February 2024.
[3] See Janneke Gerards, *General Principles of the European Convention on Human Rights* (Second edition, Cambridge University Press 2023).
[4] See Artificial Intelligence Act 2024 art 3.1.
[5] See European Parliament. Directorate General for Parliamentary Research Services., *Regulating Facial Recognition in the EU: In Depth Analysis.* (Publications Office 2021) 11 <https://data.europa.eu/doi/10.2861/140928> accessed 27 November 2023.

dactyloscopic data.[6] It often taps into Artificial Intelligence (AI) or Machine Learning (ML), enabling it to handle vast amounts of data.[7]

At this point, it is also relevant to mention that FRT is a specific type of algorithmic video surveillance system (AVS), therefore they are not exactly the same, which is why it is relevant and necessary to illustrate their differences and avoid interchanging both terms. AVS consists of an advanced video analytics software that is built into the camera and recorder, which then enables artificial intelligence functions.[8] In other words, AI can be introduced to CCTV cameras for movement detection, stranger detection, weapon and thief detection, facial recognition and so on.[9] For research purposes, in this thesis the term algorithmic video surveillance system (AVS) refers to all video algorithmic systems, excluding facial recognition technologies (FRTs). Further analysis and differentiation between both terms will be provided in following chapters.

The development and introduction of algorithm-driven technologies into society, particularly artificial intelligence (AI), algorithmic video surveillance systems (AVS) and facial recognition technologies (FRTs), have brought up diverse constitutional tensions and dilemmas. Specifically, the development of facial recognition technologies introduced the possibility for law enforcement authorities to improve their control tactics, such as surveillance.[10] The usage of FRTs has allowed for mass surveillance of the population, a development that is straight out of the novel 1984 by George Orwell.[11] A clear example of this was the seen at Südkreuz Train Station in

[6] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 art 4.14.
[7] See Konstantinos Kouroupis, 'Facial Recognition: A Challenge for Europe or a Threat to Human Rights?' (2021) 2021 European Journal of Privacy Law & Technologies 3 <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1265> accessed 26 February 2024.
[8] See Abhijit Tripathy and Vedangini Singh, 'AI-Powered CCTV Cameras Are the Future of Security and Surveillance, How Presear Softwares Deliver Advanced CCTV Video Analytics Softwares as a Hybrid Software Package Minimizing Your Cost' (Zenodo 2022) 1 <https://zenodo.org/records/6570013> accessed 30 May 2024.
[9] ibid 3.
[10] See Amy K Lehr and William Crumpler, 'Facial Recognition and Human Rights Law' (Center for Strategic and International Studies (CSIS) 2021) 3 <http://www.jstor.org/stable/resrep33749.8> accessed 27 November 2023.
[11] See George Orwell, *Nineteen Eighty-Four* (Bernard Crick ed, Clarendon Press [u.a] 1984).

Berlin, where the German Federal Police used technology to match faces in CCTV footage with high quality photos of individuals. The test lasted from 2017 to 2018 and was found to create a significant number of false positives.[12] Cases of FRT surveillance can still be seen to this day in cities such as Mannheim (Germany) where the local police installed cameras that were designed to record moving patterns of individuals, with software analysing the movement patterns for suspicious behaviour. The software reports numerous false positives, mistaking hugs for suspicious behaviour.[13]

To address these concerns, on 8 April 2019, the High-Level Expert Group on Artificial Intelligence (AI), which is an independent expert group set up by the European Commission, published its Ethics Guidelines for Trustworthy AI. [14] These guidelines had outlined seven key requirements for trustworthy AI systems: 1) human involvement and supervision; 2) technical reliability and security; 3) privacy and data management; 4) transparency; 5) non-discrimination and fairness; 6) societal and environmental welfare; and 7) accountability and responsibility. In addition to this, in 2016, the European Parliament and Council of the European Union adopted the General Data Protection Regulation (GDPR), which regulates the transfer of personal data outside the EU and EEA.[15] Furthermore, in 2020, the European Commission published a "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust" outlining policy options and regulatory adjustments to ensure safe AI development, particularly in high-risk areas impacting fundamental rights like privacy and fair trial rights.[16] Most recently, the EU has adopted the creation of the Artificial Intelligence Act (AI Act), aiming for balanced regulation to maintain technological leadership while upholding EU values and rights.

---

[12] See Greens Efa, 'Facial Recognition in European Cities - Read Our New Study' (*Greens/EFA*, 22 October 2021) <https://www.greens-efa.eu/opinions/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/> accessed 26 February 2024.

[13] ibid.

[14] See High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) 14 <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>; Also see Kaplina and others (n 5) 154.

[15] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art 1.

[16] See European Commission, 'WHITE PAPER On Artificial Intelligence - A European Approach to Excellence and Trust' 10–12 <https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf>; Kaplina and others (n 14) 155.

Due to the evolution of data collection, the EU introduced the General Data Protection Regulation to replace the 1995 Data Protection Directive used across various European countries. After the internet becomes commonplace, the EU parliament decided they need a new guideline that adapts to a more connected world where data is the common currency.[17]

On the other hand, law enforcement authorities are increasingly using AI technologies such as facial recognition systems for authentication or identification of persons involved, which creates an additional risk to the rights and freedoms of natural persons due to the processing of personal biometric data.[18] Because of this, the European Data Protection Board published the Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement[19] and Ethics Guidelines for Trustworthy AI[20], however, these are no legal binding instruments. At this point, it is necessary to mention that the EU adopted the Law Enforcement Directive (LED) since 2016, to ensure data protection. Additionally, due to the changing dynamics and the new uses of FRT it can be applicable when law enforcement authorities use this technology due to the processing of personal data (biometric data) that this technology displays, which ends up falling under the scope the mentioned directive.[21] Furthermore, even if authorities only use AI video surveillance technology, this may still go against some fundamental rights due to the constant surveillance.

However, both FRTs and algorithmic video surveillance technology (AVS) systems, due to their lack of transparency, are easy to use to identify individuals or situations without their knowledge or consent which raises privacy concerns. Furthermore,

[17] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) paras 1–5.
[18] See Balazs Gati, 'Data Protection Aspects of the Use of Facial Recognition Systems for Law Enforcement Criminal Law Section' (2023) 2023 Collection of Papers from the Conference Organized on Occasion of the Day of the Faculty of Law 306, 306.
[19] See European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf>.
[20] See 'Ethics Guidelines for Trustworthy AI' (n 14).
[21] See Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016 2016 art 2.2.

specifically FRTs pose additional concerns because, unlike other biometrics (e.g., fingerprints), facial scans can be captured easily, remotely, and secretly.[22] AVS doesn't stay behind, and since This can violate the right to privacy and family life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union (CFR) and Article 8 of the European Convention on Human Rights (ECHR).[23] This is why, the fundamental right to privacy, is crucial when referring to the application and lawfulness of FRTs and algorithmic video surveillance technologies (AVS).

The case of France is particularly interesting since France has suffered several terrorist attacks and the government has used this as a justification for the usage if FRTs as seen in the streets of Nice during the Carnival in 2019.[24] Most recently, France wanted to apply intelligent video surveillance in the Olympic Games of 2024 that will be held in Paris.[25] However, in the approved law for the Olympics, now and after refer as "Olympic Law", the use of facial recognition and cross-checking with files is prohibited after some organizations claimed it violated the right to privacy even though other forms of algorithmic video surveillance are allowed.[26]

In its Article 10, the law states that on experimental basis, until March 31, 2025, to ensure the security of large events at risk of terrorism or serious safety threats, video surveillance images may be processed using algorithms this applies to images from event venues, surrounding areas, public transport, and access roads. [27] The goal of this is to detect and report real-time events that indicate potential risks, enabling actions by

[22] See Adnan Ahmed Hafiz Sheikh, 'Facial Recognition Technology and Privacy Concerns' (21 December 2022) <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns>.
[23] See Gati (n 18) 13.
[24] See Camille Dubedout, 'Nice "Safe City" : An Acceleration of Experiments for Three Years' (*MIAI*, 24 February 2020) <https://ai-regulation.com/safe-city-project-in-nice-testing-facial-recognition/> accessed 1 March 2024.
[25] See David Charpentier, 'Paris 2024 : il y aura bien des caméras « intelligentes » pour les Jeux olympiques' (*leparisien.fr*, 23 March 2023) <https://www.leparisien.fr/jo-paris-2024/paris-2024-il-y-aura-bien-des-cameras-intelligentes-pour-les-jeux-olympiques-23-03-2023-ZUGRDLKEXJDSVD6QGXKIKBYDTM.php> accessed 1 March 2024.
[26] 'JO Paris 2024 : Comment l'intelligence Artificielle va Aider à Analyser Les Images de La Vidéosurveillance ? - France Bleu' (*ici, par France Bleu et France 3*, 16 February 2024) <https://www.francebleu.fr/infos/societe/jo-paris-2024-comment-l-intelligence-artificielle-va-aider-a-analyser-les-images-de-la-videosurveillance-1423127> accessed 1 March 2024.
[27] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) 2023 (2023-380) art 10.

national police, gendarmerie, fire and rescue services, municipal police, and the internal security services of the SNCF and Paris Transport Authority.[28] The most relevant part of the law for this research specifies that authorized operations are not permitted to use facial recognition technologies, biometric identification, or connect with other personal data systems.[29] They cannot perform any reconciliation, interconnection, or automated linking with other personal data processing. [30] They only signal predetermined events and do not independently form the basis for any individual decisions or prosecutions, maintaining human oversight throughout.[31] In other words, the use of FRTs during the 2024 Olympic Games is prohibited, meanwhile the use of AVS is allowed and encourage, in order to fulfil the security objectives proposed within the law.

Therefore, the starting point of this research will be to analyse if the proposed use of AVS in Paris during the Olympics doesn't put at risk the protection of the fundamental right to privacy as encapsulated in Article 8 ECHR and Articles 7 and 8 CFR. This is of special relevance since it is possible that in future other algorithmic video surveillance technologies will be allowed to be used and the question remains whether or under which circumstances such technologies would violate the right to privacy.[32]

II. Academic relevance of the research

After briefly addressing the legal instruments that can be linked to AVS and FRTs such as the ECHR, CFR , the GDPR, LED and the AI Act, there is a strong emphasis on adhering rigorously to the established legal frameworks, fostering transparency, ensuring accountability, and implementing robust oversight mechanisms.[33] In addition to this, scholars have also stated that a crucial aspect in understanding facial recognition

[28] ibid 10.1.
[29] ibid 10.4.
[30] ibid.
[31] ibid.
[32] See Katia Roux, '2024 Olympics: From Algorthmic Video Surveillance to Facial Recognition, There is Only One Step' (26 April 2024) <https://www.amnesty.fr/liberte-d-expression/actualites/jo-paris-de-la-videosurveillance-algorithmique-a-la-reconnaissance-faciale-il-n-y-a-qu-un-pas#:~:text=La%20reconnaissance%20faciale%20ne%20sera,ont%20m%C3%AAme%20%C3%A9rig%C3%A9%20en%20principe.>.
[33] See Asma Mekrani, 'The Future of Facial Recognition in Relation to Privacy A Research on the Added Value of the Emerging Guidance of the European Union on the Use of Facial Recognition Technologies' (Tilburg Universiy 2020) 38–43; Kouroupis (n 7) 8.

technology lies in delineating between its authentication and identification functions. Authentication is the process of verifying an individual's identity based on biometric characteristics, while identification involves matching a person's biometric data against a database to determine their identity.[34]

The debate surrounding facial recognition technology in the European Union (EU) is multifaceted, encompassing questions about its legality, ethical implications, and impact on personal data protection. Scholars have pointed out that the concerns regarding the application of FRTs on individual rights and liberties, notably privacy and data protection, are generated by the ability of these technologies to capture, analyse, and store facial biometric data.[35] This is because it raises profound concerns about potential misuse, unauthorised surveillance, and the erosion of personal privacy. A key point revolves around the perceived lack of solid legal bases for facial recognition technology in many EU Member States.[36] This critique raises pertinent questions concerning data rights, privacy, and the need for robust legal frameworks to govern the use of such technology. Scholars conclude that for addressing these concerns it is necessary to improve legal and regulatory frameworks, thereby ensuring the protection of individual rights and freedoms.[37]

Additionally, scholars have also delved into the concerns raised by the European Data Protection Supervisor regarding FRTs. This is relevant for this research because it showed that, while FRTs offer potential benefits for public safety and security, concerns persist regarding their widespread use. Issues such as error rates, algorithmic bias, and discriminatory outcomes have underscored the need for scrutiny and regulation to ensure equitable and just deployment.[38]

---

[34] See Gati (n 18) 8; 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (*European Union Agency for Fundamental Rights*, 21 November 2019) 7 <http://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 26 February 2024.
[35] See Gati (n 18); Kouroupis (n 7).
[36] See 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (n 34) 13.
[37] See Michael O'Flaherty, 'Facial Recognition Technology and Fundamental Rights Opinions' (2020) 6 European Data Protection Law Review (EDPL) 170; Gati (n 18); Kouroupis (n 7); Inez Miyamoto, 'Surveillance Technology Challenges Political Culture of Democratic States' (Daniel K Inouye Asia-Pacific Center for Security Studies 2020) <https://www.jstor.org/stable/resrep26667.9> accessed 27 November 2023.
[38] See 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (n 34).

On the other hand, some scholars have done research on AVS tools, and some have concluded that although AVS doesn't process the same kind of data like FRTs, these tools can also represent a risk to the right to privacy and personal data.[39] Additionally, according to other scholars, the issue with privacy relies within the massive collection of biometric data that FRT allows.[40] On the same line, different authors tend to approach the concept of AVS only from the FRTs perspective[41], which has created a gap in the research and analysis of this technology.

In addition to this, as we have seen, the new EU Artificial Intelligence Act represents a significant step toward addressing regulatory gaps and limiting the use of biometric identification systems, including FRTs. However, most of the literature efforts on FRTs does not analyse this new instrument.

Considering the available literature about the application of FRTs and AVS for mass surveillance in public spaces, there seems to be a gap upon the concrete differences between both types of technologies and the possible effects that the new AI Act may bring upon these technologies. In addition to this, case studies as will be described in my thesis are relevant since these represent the usage of FRTs in the real world and its real-time implications upon fundamental rights such as the right to privacy. Therefore, there is an opportunity to analyse this real practice case studies and verify their lawfulness and compliance in terms of and the HDPR, the LED and the new AI Act.

As mentioned earlier, the case of France is particularly interesting since France wanted to use AI to effectively assist the massive security risks that hosting the 2024 Olympic Games implies.[42] However, in the approved law for the Olympics, the use of facial recognition and cross-checking with files is prohibited.[43] Even though it was prohibited for the Olympic Games, some sectors claim that France has strong mobilization against

[39] See Ezgi Turgut Bilgic, 'Personal Data Protection in the Context of Video Surveillance in Public Areas: The Case of France' (2023) 13 Hacettepe Hukuk Fakultesi Dergisi 414, 416; See also Mark D Cole, 'Recent Developments and Overview of the Country and Practitioner's Reports Reports: Introduction' (2020) 6 European Data Protection Law Review (EDPL) 94, 96.
[40] See Roux (n 32).
[41] ibid; See also Turgut Bilgic (n 39); Antonina Semivolos, 'The Advent of Facial Recognition and the Erosion of the Rule of Law in "Moscow Smart City"' (2022) 29 Cardozo Journal of Equal Rights and Social Justice 345.
[42] See Charpentier (n 25).
[43] 'JO Paris 2024 : Comment l'intelligence Artificielle va Aider à Analyser Les Images de La Vidéosurveillance ? - France Bleu' (n 26).

the ban on facial recognition at European level during the debates on the European Union regulation on AI (AI Act)[44]. Therefore, it seems like this prohibition was initially done just to avoid any backlash from the public, which might raise the concern if this prohibition is enough to protect the right to privacy as encapsulated in Article 8 ECHR and Articles 7 and 8 CFR, since the deployment of other types of AVS are allowed.

III. Research Question

In this thesis, I will analyse the legal limitations that FRT has when used for mass surveillance for identifying and categorizing individuals in Paris, France, during the Olympic Games of 2024. I will apply the ECHR, CFR, GDPR, LED and the AI Act to conclude if this FRT limitations should also be applied to the use of AVS in order to protect the right to privacy of individuals. The main research question of this thesis is as follows:

'Are the legal limitations on Facial Recognition Technologies under Articles 8 ECHR, Article 7 CFR, the GDPR, the LED, and the AI Act, equally applicable to Algorithmic Video Surveillance systems used during the 2024 Paris Olympic Games?'

In order to dive into a complete analysis, I propose the following sub questions to be solve as well:

1) What are the fundamental characteristics of facial recognition technologies (FRT) and algorithmic video surveillance (AVS) technologies as proposed for the Olympic Games?
2) What are the main differences between FRT and AVS technologies?
3) What does the Olympic Law state in terms of the deployment of AVS and the prohibition of FRTs?
4) What are the legal limitations concerning the use of FRT and AVS in public spaces on the basis of the right to private life as protected under Article 8 ECHR and Article 7 CFR?
5) What are the legal limitations concerning the use of FRT and AVS on the basis of the GDPR, LED, and the new AI Act?

[44] See Roux (n 32).

IV. Methodology and Perspective

In order to provide a complete research and analysis, different sources and methods will be used to answer the research question. Mainly, doctrinal legal research will be employed with the aim of providing enlightenment on the controversial aspects of mass surveillance and its effect on privacy protection. I have opted for a single case study because it will allow me to generate an in-depth analysis and will also allow me to delimitate the scope of the study. To describe the case study, I will be referring to French legislation, parliamentary documents and reports by the CNL and NGO's. Additionally, since by the time of writing of this thesis the case study is still ongoing and this limits my sources of research, I will also use various news articles and blogposts about the case to be able to provide a full description of the case.

Doctrinal legal research will be used to better comprehend the background and the specific information contained in this thesis. Terms like Algorithmic video surveillance technologies (AVSs), FRTs, AI, algorithms, the fundamental right to privacy and so, are only able to be explained when looking into research reports of EU institutions and academic articles with the aim of giving a systematic exposition of the principles, rules and concepts governing the use of AIVS and FRTs for mass surveillance in public spaces. In addition, this will also help to analyse the relationship between these principles, rules and concepts with a view to solving unclarities and gaps in the existing regulations.

This study will be conducted from a fundamental rights perspective, focusing on the right to privacy. Legal normative research will also be applied since it is necessary to investigate sources of law such as the European Convention on Human Rights, Charter of Fundamental Rights of the European Union, Law Enforcement Directive and the proposed AI Act. In addition to this, I will also investigate applicable case law from the European Court of Human Rights (ECtHR) on the basis of Article 8 ECHR and the Court of Justice of the European Union concerning Articles 7 and 8 CFR and the GDPR and LED applications. Hereby, I will map the legal framework based on Article 7 CFR on the respect for private and family, while also delving into Article 8 of the CFR on data protection.

V. Chapter overview

In Chapter 1, I will provide the main characteristics of Facial Recognition Technologies, in order to understand better this technological system. I will also provide the main differences of FRTs with Traditional Video Surveillance since this can help to the full comprehension of the term FRTs. Additionally, I will present all the information related to the type of data and the processing of data collected by FRTs. In Chapter 2, I will provide the main characteristics of Algorithmic Video Surveillance technologies, since this is fundamental to understand better this technological system. I will also provide the main differences of AVS with FRTs. I will present this chapter based on the usage intended for AVS at the Paris Olympic Games 2024.

In Chapter 3 I will discuss the objectives, scope, and content of the Olympic Law, as well as the constitutional validity of the law and the operational deployment and testing of AVS. Furthermore, in Chapter 4, this chapter will define the concept of privacy and explore the legal instruments related to the right to privacy, including relevant case law on FRTs and video surveillance**.**

In Chapter 5 I will examine key provisions in the General Data Protection Regulation, the Law Enforcement Directive and the Artificial Intelligence Act in order to provide the legal limitations on the use of FRT. Finally, Chapter 6 will examine whether the legal limitations of FRT should also apply to AVS and how these ones could be applied.

Chapter 1: Characteristics of Facial Recognition Technologies (FRT) and its Distinctions from Traditional Video Surveillance

1.1 Introduction

The Olympic Law marks a significant development in the application of artificial intelligence (AI) for security purposes, setting a legal framework that aims to protect fundamental and individual freedoms while enhancing public safety.[45]One of the key provisions of the Olympic Law is the explicit prohibition of facial recognition

[45] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) 10.1.

technologies (FRT) and any form of cross-checking with existing databases.[46] This decision was influenced by concerns over privacy violations, voiced by various sectors, which argued that FRT could infringe on the right to privacy as enshrined in Article 8 of the ECHR Articles 7 and 8 of the CFR.[47] Despite this prohibition, other forms of AI-powered video surveillance have been permitted, raising questions about the overall sufficiency of these measures in safeguarding privacy rights.[48] Before going into further detail about the content of the Olympic Law, it is necessary and relevant explain the main characteristics and differences of FRTs and AVS.

1.2 Development and Introduction of Facial Recognition Technologies (FRTs)

Facial Recognition Technology (FRT) represents a significant advancement in the field of surveillance, offering the ability to identify and track individuals based on their unique facial features.[49] As proposed in France for the Olympic Games 2024, FRT has been considered for mass surveillance applications, raising controversial questions about privacy, security, and the ethical implications of its deployment.

Facial recognition technology has undergone significant advancement since its introduction in the early 1990s. Additionally, its commercialization gained momentum in the 2000s with the development of larger, more complex datasets.[50] Furthermore, the integration of deep learning techniques from 2014 onwards has propelled its evolution even further. FRT is a subset of biometric technologies, which encompass a variety of technologies serving different functions, spanning from the basic detection of a face in an image to more intricate tasks such as verification, identification, and categorization or classification of individuals.[51] First, the identification feature consists on the comparison of a person's facial image with other templates stored in a database to

[46] See Ministry News, 'Lancement de l'expérimentation « vidéo-intelligentes » en vue de la sécurisation des Jeux Olympiques | Ministère de l'Intérieur et des Outre-mer' (19 April 2024) <https://www.interieur.gouv.fr/actualites/actualites-du-ministere/lancement-de-lexperimentation-video-intelligentes-en-vue-de> accessed 31 May 2024.
[47] See Roux (n 32).
[48] ibid.
[49] See Kouroupis (n 7) 151.
[50] See European Parliament. Directorate General for Parliamentary Research Services. (n 5) 1–2.
[51] See Directorate-General for Parliamentary Research Services (European Parliament), Tambiama Madiega and Hendrik Mildebrath, *Regulating Facial Recognition in the EU: In Depth Analysis* (Publications Office of the European Union 2021) 1 <https://data.europa.eu/doi/10.2861/140928> accessed 26 February 2024.

discover if their image is stored there.[52] Second, the verification feature consists of a comparison of two biometric templates, assumed to belong to the same person, to check if both images contain the same identity or if they match.[53] Finally, the categorisation or classification feature consists of extracting features from the facial image to determine different attributes such as age, gender, race, or emotional state[54].

In the context of mass surveillance, FRTs offers the ability to track the movement of individuals in public spaces,[55] monitor crowds,[56] and even identify persons of interest in real-time[57]. This capability has raised concerns about the potential for governments and companies to do invasive surveillance practices that can violate privacy rights.

1.3 Distinctions from Traditional Video Surveillance

While traditional video surveillance systems rely on capturing and recording visual images for retrospective analysis,[58] FRT introduces a proactive and automated approach to identifying individuals in real-time using biometric data.[59] Biometric data can be understood as personal data obtained from specific technical processing of an individual's physical, physiological, or behavioural characteristics, such as facial images or fingerprint data.[60] Unlike traditional surveillance cameras, which primarily serve as passive observers, FRT systems actively analyse and interpret the data they capture, enabling rapid identification and classification of individuals based on their facial features[61].

---

[52] See European Parliament. Directorate General for Parliamentary Research Services. (n 5) 1–2.
[53] ibid.
[54] ibid.
[55] See Sara Solarova and others, 'Reconsidering the Regulation of Facial Recognition in Public Spaces' (2023) 3 AI and Ethics 625, 626.
[56] See Mark Packulak, 'Who Watches the Watchers: Oversight of State Surveillance' (2022) 45 Manitoba Law Journal 101, 113–114.
[57] ibid.
[58] See Ray Surette, 'The Thinking Eye - Pros and Cons of Second Generation CCTV Surveillance Systems' (2005) 28 Policing: An International Journal of Police Strategies and Management 152, 158–159.
[59] See European Parliament. Directorate General for Parliamentary Research Services., *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues.* (Publications Office 2021) 13 <https://data.europa.eu/doi/10.2861/91831> accessed 17 April 2024.
[60] Artificial Intelligence Act art 3 (34).
[61] Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial Recognition in Online and Mobile Services' 2 <https://www.pdpjournals.com/docs/87997.pdf>.

Moreover, FRT's capability to perform biometric authentication allows for the verification of individuals' identities with a high degree of accuracy[62]. This contrasts with the traditional video surveillance, which typically relies on manual review and interpretation of footage by humans.[63] In addition to this, FRT systems have the potential to be deployed at scale across diverse environments, including public spaces, transportation hubs, and commercial establishments.[64] This widespread adoption can amplify the reach and the impact of surveillance activities, raising concerns about the potential for mass surveillance and its implications for civil liberties.[65]

1.4 Collection of Biometric Data through FRTs

The core of FRT systems is the collection and processing of biometric data, specifically facial images. Unlike other forms of biometric data, such as fingerprints or iris scans, facial images can be captured non-invasively and from a distance, making them particularly suited for surveillance applications.[66] The collection of biometric data through FRTs raises unique privacy and data protection concerns as illustrated in Recital 51 of the GDPR.[67] Facial images are inherently sensitive personal data, as they can reveal a lot of information about an individual, including their identity, emotions, and activities.[68] Furthermore, the widespread deployment of FRT systems increases the risk of unauthorized access to biometric data, potential misuse, and the creation of comprehensive profiles of individuals without their consent.[69]

---

[62] ibid 1.
[63] Surette (n 58) 157–158.
[64] See Joy Buolamwini and others, 'Facial Recognition Technologies: A Primer' 7–8 <https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf>.
[65] Gati (n 18) 324.
[66] See European Parliament. Directorate General for Parliamentary Research Services. (n 59) 28.
[67] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) para 51.
[68] See 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (n 34) 5.
[69] European Parliament. Directorate General for Parliamentary Research Services. (n 5) 6–8.

1.5 Conclusion

In summary, FRTs represent a paradigm shift in surveillance capabilities, offering unprecedented opportunities for identification, tracking, and analysis of individuals in public spaces. Distinguished from traditional video surveillance methods by its proactive and automated approach, FRT introduces unique challenges and considerations related to privacy, data protection, and regulatory compliance. Understanding the fundamental characteristics of FRT, its distinctions from traditional surveillance methods, and the implications of its usage for mass surveillance is essential for informed policy-making and the protection of fundamental rights in the digital age.

Chapter 2: Characteristics of Algorithmic Video Surveillance Technologies: A Proposal for the Olympic Games in France

2.1 Introduction

AI video surveillance represents a novel approach to monitoring and analysing public spaces, especially in the context of large-scale events such as the Olympic Games. In Case of the Olympic Games of 2024 in France, the adoption of AI-assisted video surveillance reflects the intersection of technology, security, and privacy concerns. This chapter aims to explore the fundamental characteristics of AI video surveillance technologies as proposed for the Olympic Games in France and to delineate the key differences between AI video surveillance technologies (AVS) and Facial Recognition Technologies (FRT).

2.2 Main Characteristics of AI Video Surveillance Technologies

Algorithmic video surveillance technologies tend to offer a wide range of sophisticated analytical functions, such as theft detection, vehicle and face recognition, person identification, people and traffic counting, weapons detection, and behavioural analytics.[70] In other words, AVS involves the use of artificial intelligence (AI) algorithms to analyse live or recorded video feeds from surveillance cameras,

[70] See 'AI in Video Surveillance | Isarsoft' (19 September 2023) <https://www.isarsoft.com/article/ai-in-video-surveillance> accessed 5 July 2024.

enhancing the surveillance capabilities of traditional video surveillance.[71] As it was already mentioned, these algorithms can perform various tasks, including object detection, accident detection, and illegal activity detection, without the need for human intervention.

In the case of the Olympic Games of 2024 in Paris, France adopted Law no. 2023-380 of May 19, 2023 relating to the 2024 Olympic and Paralympic Games and containing various other provisions. With this law, France authorizes, for the first time, the implementation of artificial intelligence solutions in video protection.[72] This has been understood as an experiment that aims to explore the potential of ethical and trustworthy artificial intelligence while enhancing the security of major events by supporting, not replacing, traditional video surveillance operators.[73]

As it was already mentioned, traditional video surveillance provides real-time images for better situational awareness, but the volume of footage can end up overwhelming human operators.[74] By integrating AI with traditional systems, this initiative aims to improve the detection of unusual situations in order to help human operator take better informed decisions.[75] Operators will maintain control over alerts and decide when to escalate issues for further action.[76]

From August to December 2023, the Ministry of the Interior and Overseas Territories rigorously evaluated AVS for their technical performance and compliance with ethical standards. Wintics' co-director Matthias Houllier noted that while the technological base has been widely tested for statistical purposes, the Olympic context introduces a new aspect: triggering alerts when statistics exceed certain thresholds.[77] This

[71] See Ben Bowling and Shruti Iyer, 'Automated Policing: The Case of Body-Worn Video Special Issue on Law, Liberty and Technology: Criminal Justice in the Context of Smart Machines' (2019) 15 International Journal of Law in Context 140.
[72] Ministry News (n 46).
[73] Laure Gamaury, 'Aux JO, de la vidéosurveillance sans reconnaissance faciale, vraiment ?' (*www.20minutes.fr*, 4 March 2024) <https://www.20minutes.fr/sport/jo_2024/4077797-20240304-jo-paris-2024-videosurveillance-reconnaissance-faciale-vraiment> accessed 31 May 2024.
[74] Ministry News (n 46).
[75] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 10.
[76] ibid.
[77] Gamaury (n 73).

repurposing of the technology raises concerns about facial recognition, a currently banned process, re-entering the debate when discussing AI-powered cameras.[78]

Since 2017, Wintics' software, which won two Ministry of the Interior tenders for communities and transport, has been used to transform videos into statistical data.[79] For example, it has been utilized to quantify bicycle use and regulate traffic lights in Paris. However, the JO law, adopted in spring 2023, particularly Article 7, expands this software's capabilities to send real-time alerts to security operators when predefined thresholds are exceeded for eight types of events[80]:

- Failure to respect the direction of traffic
- Crossing a prohibited area
- The presence or use of a weapon
- An outbreak of fire
- A crowd movement
- One person on the ground
- Too much density
- An abandoned package[81]

The Wintincs' AVS software for the Olympic Games of Paris claims it will not collect biometric data nor personal data. AVS identifies and recognizes silhouettes, but also assures that it does not store "neither images nor videos".[82] Therefore, AVS in the Paris Olympic Games of 2024 will be understood as software that is not able to have any information relating to an identified or identifiable natural person, because it doesn't collect any personal data[83].

[78] ibid.
[79] ibid.
[80] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 7.
[81] Gamaury (n 73).
[82] ibid.
[83] See Othman O Khalifa and others, 'Video-Based Abnormal Behaviour Detection in Smart Surveillance Systems' in Khalid Isa and others (eds), *Proceedings of the 12th National Technical Seminar on Unmanned System Technology 2020* (Springer 2022) 329.

2.3 Differences with Facial Recognition Technologies (FRTs)

While Algorithmic video surveillance technologies (AVSs) share some similarities with Facial Recognition Technologies (FRTs), there are key differences between them, as recognized already by the French government in the Olympian Law. First and foremost, AVS focuses on analysing overall patterns of behaviour and detecting anomalies or suspicious activities within a broader context.[84] In contrast, FRT specifically targets the identification and verification of individual faces within a crowd, often for the purpose of biometric authentication or tracking.[85]

Second, the most important difference between the two technologies relies on the level of intrusiveness. AVS operates at a more macroscopic level, analysing aggregate data from multiple sources to identify potential threats or security risks. Specifically, Matthias Houllier, co-director of Wintics, states that their AVS identifies and recognizes silhouettes, but also assures that it does not store "neither images nor videos".[86] In other words, they argue their software doesn't process or collect any biometric data, as it was stated in the law that it is prohibited to use any technology that collects or process biometric data nor personal data.[87] On the other hand, FRT, involves the collection and processing of highly personal and identifiable biometric data, raising greater concerns about privacy and civil liberties.[88]

Additionally, one could argue that there is another difference between both technologies, which consist of the purpose of deployment. On the one hand, AVS is typically deployed for general security and safety purposes, such as crowd management, perimeter protection, and incident detection.[89] Meanwhile, FRT is often used for targeted surveillance or law enforcement purposes, raising additional ethical and legal considerations.[90] Because of this, both AVSs and FRTs are subject to regulatory frameworks governing privacy and data protection since FRT is subject to

[84] ibid.
[85] See Directorate-General for Parliamentary Research Services (European Parliament), Madiega and Mildebrath (n 51).
[86] Gamaury (n 73).
[87] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 10.4.
[88] See European Parliament. Directorate General for Parliamentary Research Services. (n 59) 13.
[89] Gamaury (n 73).
[90] See 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (n 34) 1–3.

more stringent regulations due to its potential for intrusive surveillance and the collection of sensitive biometric data.[91]

2.4 Conclusion

In conclusion, by leveraging artificial intelligence algorithms to analyse video feeds in real-time, algorithmic video surveillance systems can detect and respond to potential threats or security risks more effectively. However, it is essential to recognize the differences between AVS and FRT, particularly in terms of the level of intrusion, the focus of analysis, and the regulatory framework governing their usage. By understanding these distinctions and implementing appropriate safeguards, policymakers can ensure that AVS enhances security without unduly compromising individual privacy rights.

Chapter 3: France's rejection of Facial Recognition Technologies but going hand in hand with Algorithmic video surveillance technologies in the Olympic Games in Paris of 2024.

3.1 Introduction

To address the security challenges that hosting the Olympic Games creates, France has authorized the use of algorithmic video surveillance (AVS) under the law of May 19th, 2023, commonly referred to as the "*JO loi*" or in English "Olympic Law".[92] This law marks a significant development in the application of artificial intelligence (AI) for security purposes, setting a legal framework that aims to protect fundamental and individual freedoms while enhancing public safety. [93] This chapter aims to describe the content of the law that is related to the allowance of AVS and the prohibition of FRT as security measures for the massive event.

[91] Gati (n 18) 312.
[92] 'JO 2024 Loi du 19 mai 2023 Jeux Olympiques et Paralympiques | vie-publique.fr' <https://www.vie-publique.fr/loi/287639-jo-2024-loi-du-19-mai-2023-jeux-olympiques-et-paralympiques> accessed 31 May 2024.
[93] ibid.

3.2 Objectives, scope and content of the JO Law

Following a first law of 2018, the Olympic Law it completes the legislative arsenal put in place to enable the smooth running of the French territory for the 2024 Olympic and Paralympic Games.[94] The primary objective of this legislative experiment is to explore the potential contributions of AI, which is designed to be ethical and trustworthy, to the security of major events.[95] The law aimed to facilitate the work of operators of traditional video protection devices without replacing human judgment. The coupling of algorithmic processing with traditional video protection is expected to enhance the ability to detect unusual situations, thus improving the overall security apparatus.[96]

Even from the first debate of the draft of what would become to be Law No. 2023-380 of 19 May 2023, Senators highlighted the magnitude of the sports event, with 15,000 athletes, media, with more than four billion viewers, and organizational, with the equivalent of forty-three world championships.[97] The law covers diverse topics from creation of a Olympic and Paralympic village medical attention to antidoping, however, for this research, I will mostly focus on Chapter III and other dispositions related to the security measures that will be deployed during the 2024 Olympic Games in Paris.

Now, I proceed to explain in depth the research-relevant articles of the Olympic Law. Chapter III of the law contains provisions aimed at better guaranteeing security from articles 9 to 19. For starters, Article 9 amends Article L. 223-1 and Article L. 251-2 by adding to the first line that "Video surveillance systems can be implemented on public roads by the authorities…".[98] Additionally, the third point of Article 9 amends Art. L. 251-1.- stating that "Video protection systems meeting the conditions set out in Article L. 251-2 are processing of personal data governed by this title, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

[94] Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 'La Lettre de la DAJ – La loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions' (8 June 2023) <https://www.economie.gouv.fr/daj/la-lettre-de-la-daj-la-loi-relative-aux-jeux-olympiques-et-paralympiques-de-2024> accessed 21 June 2024.
[95] ibid.
[96] Ministry News (n 46).
[97] Sénat, 'Séance du 24 janvier 2023' (2023) <https://www.senat.fr/seances/s202301/s20230124/s20230124011.html#Niv1_SOM9> accessed 22 June 2024.
[98] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 9.1(a); ibid 9.4(b).

protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general regulation on the protection of data) and by Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms."[99]

Finally, Article 9 also amends Art. L. 255-1. Which now states that: "The terms of application of this title and use of data collected by video protection systems are specified by a decree in the Council of State, taken after consultation with the National Commission for Informatics and freedoms. This decree sets out the conditions under which the public is informed of the existence of processing of personal data by a video protection system and the manner in which data subjects can exercise their rights under the European Regulation (EU) 2016 /679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation general on data protection) and Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms."[100]

Meanwhile, Article 10 describes an experimental program authorized until March 31, 2025, for using algorithmic processing of video (AVS) images to enhance security at large-scale events exposed to terrorism or serious safety threats. The program aims to detect, and report predetermined events in real time using video protection systems at event locations, surrounding areas, public transport vehicles, and access roads, supporting national police, fire and rescue services, municipal police, and internal security services of the SNCF and the Régie Autonome des Transports Parisiens.[101]

Governed by strict legal and ethical frameworks, the operations described in this article comply with the EU General Data Protection Regulation (GDPR) and French data protection laws.[102] Additionally, public notification of the use of algorithmic processing on images collected by means of video protection systems authorized on the basis of article L. 252-1 of the internal security code and cameras installed on aircraft authorized

[99] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 9.3.
[100] ibid 9.15.
[101] ibid 10.1.
[102] ibid 10.2.

on the basis of Chapter II of Title IV of Book II of the same code, except when circumstances prohibit it or this information would conflict with the objectives pursued.[103] The systems are prohibited from using biometric identification, facial recognition (FRT), or linking with other personal data processing systems. They are solely for signalling specific events without making individual decisions or initiating prosecutions independently, maintaining human oversight.[104]

The use of AVS systems will be authorized by decree taken after advice from the National Commission for Information Technology and Liberties (CNIL). A public consultation on this decree may be organized by the government.[105] The decree must outline the system's characteristics, events to be detected, special circumstances justifying its use, authorized services, financial contributions, and agent training conditions, while also including a data protection impact analysis to evaluate benefits, potential risks, and risk management measures.[106]

It is also stated in Article 10 that the State oversees the system's development, potentially delegating it to a third party while ensuring compliance with cybersecurity requirements.[107] The system must meet criteria for training data relevance, traceability, human control measures, and operational interruption conditions. Additionally, a test phase must be conducted and certified, while third-party developers must provide technical documentation and guarantees of competence, continuity, assistance, and human control to address errors or biases.[108]

Furthermore, State representatives in respective departments or the prefect of police in Paris must authorize the system's use, with each authorization being public, reasoned, and limited to one month, renewable if conditions are met.[109] Public implementation must be informed, and system operations must be regularly reported to relevant authorities, with weekly updates for state representatives and periodic updates for local

[103] ibid 10.3.
[104] ibid 10.4.
[105] ibid 10.5.
[106] ibid 10.
[107] ibid 10.6.
[108] ibid.
[109] ibid 10.7.

mayors and the CNIL.[110] The article also provides that the authorization for the AVS use may be suspended or terminated if initial conditions are no longer met.[111]

In addition to this, for system improvement, the article provides that a sample of collected images may be used for training data for up to twelve months under strict conditions, ensuring relevance and security, while the CNIL monitors the experiment to ensure compliance with data protection laws and reports findings to the government.[112] For monitoring purposes, an evaluation report on the experiment, involving public and agent feedback, will be submitted to Parliament by December 31, 2024, and made public online.[113]

3.3 Constitutional validity of the Olympic Law

It is also relevant to mention at this point that the Constitutional Council was referred to the law concerning the 2024 Olympic and Paralympic Games, along with various other provisions on May 17 of 2023 (two days before the adoption of the Olympic Law). The petitioning deputies challenged the constitutionality of several articles of the law. However, according to Article 61 of the Constitution, only texts that have the status of laws can be referred to the Constitutional Council.[114]

The Constitutional Council reviewed provisions related to the allowance of algorithmic processing of images from AVS to detect specific events, aiming to prevent public order breaches. Once again, the Council states that it is necessary authorization for such processing, aimed at enhancing event security, requires justification by state representatives and must be proportionate.[115] It is also stated that the processing cannot modify image collection conditions but significantly enhances information precision.[116]

[110] ibid 10.8.
[111] ibid.
[112] ibid 10.9.
[113] ibid 10.10.
[114] *Décision n° 2023-850 DC du 17 mai 2023 | Conseil Constitutionnel* [2023] Conseil Constitutionnel 2023-850 [1–2].
[115] ibid 38.
[116] ibid 33.

Therefore, the implementation of such surveillance systems must be accompanied by specific guarantees likely to safeguard the right to respect for private life.[117]

In order to prevent certain breaches of public order, article L. 252-1 of the internal security code provides that the prefect may authorize the installation of video protection systems on public roads or in places open to the public.[118] These measures aim to secure events at risk of terrorism or severe security threats, excluding minor risks. After careful consideration, the Council considers that the legislature balanced security needs with privacy rights, ensuring legal oversight and procedural fairness.[119]
Furthermore, Article 13 extends AVS access for security agents, with strict controls to prevent privacy violations. The Council emphasized the importance of clear regulations and training requirements for agents accessing these images, in order to harmonize security imperatives with privacy protections, promoting accountability and compliance with legal standards.

Finally, the Constitutional Council, in its decision 2023-850 DC, confirmed the constitutional validity of AVS processing, provided that it is accompanied by specific safeguards to protect the right to private life.[120] These safeguards include prior public information, human oversight measures, risk management systems, and oversight by the National Commission for Information Technology and Liberties (CNIL). [121]

3.4 Operational Deployment and Testing

The Olympic Law established the requirement of testing the usage of AVS before the Olympic Games, which is why the initial testing phase of these AI tools was conducted during various public events, such as the Dépêche Mode concert at Arena Bercy and the Paris-Nancy basketball match at Adidas Arena.[122] On March 5, 2024, the first test of algorithmic video surveillance (AVS) technology took place during a the Dépêche Mode concert at the Accor Hotel Arena in Bercy. Six cameras equipped with AVS from

[117] ibid 32–39.
[118] ibid 34.
[119] ibid 44–49.
[120] ibid 49.
[121] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 10.4.
[122] Ministry News (n 46).

Wintics -a Parisian company awarded several prizes for the Olympic Games- were deployed around the hall by the Paris police headquarters. The Ministry of the Interior clarified that the cameras were intended to test and configure software solutions in real conditions, not to detect events or make arrests.[123]

The operational phase then began in April 2024, involving the deployment of 100 cameras by the RATP during the Black-Eyed Peas concert at La Défense Arena, and 118 cameras by the SNCF during the PSG-Olympique Lyonnais match.[124] These cameras are equipped with automated image analysis solutions designed to detect predetermined security events, such as the presence of abandoned objects, unauthorized access to sensitive areas, crowd movements, and high crowd density.[125]

3.5 Conclusion

The legal framework established by the JO law reflects a cautious yet progressive approach to integrating AI into public safety measures. While facial recognition remains prohibited, the deployment of other AI-driven surveillance technologies raises important questions about privacy and civil liberties. The forthcoming CNIL doctrine and the independent evaluation report will play crucial roles in shaping the future application of AI in public surveillance beyond the Olympic Games.

Chapter 4: Legal Framework on the Right to Privacy and Usage of Facial Recognition Technology

4.1 Introduction

The right to privacy is a fundamental human right enshrined in various legal instruments, including the Charter of Fundamental Rights of the European Union (CFR) and the European Convention on Human Rights (ECHR). In the context of restricting the power of national authorities to observe their inhabitants permanently within public areas, Article 8 of the ECHR and Article 7 and 8 of the CFR play pivotal

[123] Gamaury (n 73).
[124] Ministry News (n 46).
[125] Gamaury (n 73).

roles. This chapter explores the components of the right to privacy, analyses key provisions outlined in Article 8 of the ECHR and Article 7 and 8 of the CFR and the relevant case law related to video surveillance and/or facial recognition technologies.

4.2 Defining the Concept of Privacy

Privacy is a multifaceted concept that encompasses various aspects of individual autonomy, dignity, and control over personal information.[126] It includes the right to be left alone, the right to control one's personal data, and the right to engage in activities without unwarranted intrusion or surveillance. Privacy is fundamental to the preservation of individual autonomy, the protection of intimate relationships, and the maintenance of democratic societies[127].

4.3 Legal Instruments on the Right to Privacy

4.3.1 Article 8 of the ECHR and Relevant Case Law on Video Surveillance and/or Facial Recognition

First, Article 8 of the ECHR provides that everyone is entitled to respect for their private and family life, home, and correspondence.[128] Additionally, it is also stated that public authorities shall not interfere with this right unless such interference is lawful and necessary in a democratic society for the interests of national security, public safety, economic well-being, prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others.[129] This obligation is a classic negative duty, considered the essential object of Article 8.[130] Although Article 8 primarily protects individuals from public authority interference, it not only requires the State to

[126] See Jackson Adams and Hala Almahmoud, 'The Meaning of Privacy in the Digital Era' (2023) 15 International Journal of Security and Privacy in Pervasive Computing (IJSPPC) 1, 2.
[127] See Jonathan Kahn, 'Privacy as a Legal Principle of Identity Maintenance' (2002) 33 Seton Hall Law Review 371, 401–402.
[128] See Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) [hereinafter: ECHR], art. 8.1.
[129] ECHR, art. 8.2.
[130] See *Kroon and Others v the Netherlands* [1994] ECtHR 19016/18, 56976/18, 41405/21, 56248/21, 56279/21, 57904/21, 61341/21, 12360/22, 30061/22, 38307/23 [31].

refrain from such interference but also imposes positive obligations to ensure effective respect for private life.[131]

Furthermore, in terms of the scope of Article 8, it is relevant to mention that the European Court of Human Rights (ECtHR) notes that the concept of "private life" is a broad term not susceptible to exhaustive definition.[132] It is a concept which covers the physical and psychological integrity of a person and can embrace multiple aspects of the person's physical and social identity, therefore not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle.[133] The Court has also held that everyone has the right to live privately, away from unwanted attention.[134]

The Court has determined that video surveillance of public places, where the visual data is recorded, stored, and disclosed to the public, falls under Article 8.[135] Additionally, video surveillance in workplaces, like supermarkets[136] and university amphitheatres also falls within Article 8's scope.[137] In relation to this and in terms of data protection, it is stablished that the protection of personal data is crucial for enjoying the right to respect for private and family life under Article 8 ECHR, even if than information is already in the public domain.[138] Article 8 ECHR grants individuals the right to informational self-determination, allowing them to claim privacy rights over data that, although neutral, is collected, processed, and disseminated in ways that may engage their Article 8 rights.[139]

---

131 *Lozovyye v Russia* [2018] ECtHR 4587/09 [36].
132 See *Khadija Ismayilova v Azerbaijan* [2019] ECtHR 65286/13, 57270/14 [139].
133 ibid.
134 ibid; See also *Smirnova v Russia* [2003] ECtHR 46133/99, 48183/99 [95]; *Bărbulescu v Romania* [2017] ECtHR [GC] 61496/08 [70].
135 See *Peck v the United Kingdom* [2003] ECtHR 60898/00 [57–63]; *Glukhin v Russia* [2023] ECtHR 11519/20 [67].
136 See *López Ribalda and Others v Spain* [2019] ECtHR [GC] 1874/13, 8567/13 [93].
137 See *Antović and Mirković v Montenegro* [2017] ECtHR 70838/13 [41–45].
138 See *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECtHR [GC] 931/13 [133–134]; *L.b v Hungary* [2023] ECtHR [GC] 36345/16 103–104.
139 See *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (n 138) paras 133–134; *L.b. v. Hungary* (n 138) 103–104.

Additionally, it is relevant for the research to mention that the Court considers a person's image a fundamental part of their personality, essential for personal development.[140] More specifically, it is also stablished that the State has positive obligations to ensure efficient criminal or civil laws that prohibit non-consensual filming. In *Söderman v. Sweden*, 2013, a 14-year-old girl's stepfather attempted to covertly film her while she was naked. Her complaint highlighted that Swedish law at the time did not prohibit such filming, failing to protect her personal integrity.[141] Similarly, in *Khadija Ismayilova v. Azerbaijan*, 2019, a journalist was covertly filmed inside her home, and the videos were publicly disseminated. Although the acts were criminalized and proceedings began, the Court found that the authorities failed in their positive obligation to effectively investigate the serious violations of her private life.[142]

In terms of police surveillance, in *Glukhin v. Russia*, 2023, the Court addressed police use of facial recognition technology for the first time. FRT identified the applicant from public photographs and videos on Telegram and this was then used to locate and arrest him. The Court highlighted the intrusive nature of these measures, requiring a high level of justification to be considered "necessary in a democratic society", with live facial recognition demanding the highest justification.[143] The applicant had been prosecuted for a minor offence of holding a solo demonstration without prior notification, without any accusations of causing public danger or committing reprehensible acts. Given these circumstances, the Court concluded that using facial recognition technology, especially live technology, did not meet a "pressing social need" and was not "necessary in a democratic society", representing a violation of Article 8 ECHR.[144]

Based on the information previously presented, there are various legal limitations on the use of Facial Recognition Technology (FRT) under Article 8 ECHR. First, in terms of material limitations, Article 8 provides protection to individuals from using FRTs for arbitrary interferences by public authorities. [145] Second, the same article also encapsulates the limitation of positive obligations of States, which consist of ensuring

[140] *López Ribalda and Others v. Spain* (n 136) paras 87–91.
[141] See *Söderman v Sweden* [2013] ECtHR [GC] 5786/08 [40, 105].
[142] See *Khadija Ismayilova v. Azerbaijan* (n 132) para 112.
[143] See *Glukhin v. Russia* (n 135) para 86.
[144] ibid 88–90.
[145] See *Libert v France* [2018] ECtHR 588/13 [40–42]; *Drelon v France* [2022] ECtHR 3153/16, 27758/18 [85].

the effective respect for private life, which includes enacting laws to prevent non-consensual filming and ensuring efficient investigation of violations on the usage of FRTs, in this specific case of the Olympic Games.[146] Third, the broad scope of "private life" under Article 8 ECHR imposes material limitations on the use of FRT by protecting various dimensions of individual autonomy and identity.[147] It ensures that FRT is used judiciously, with careful consideration of its impact on individuals' physical, psychological, and social well-being. [148] This broad interpretation acts as a safeguard against potential abuses of FRT, maintaining a balance between technological advancements and fundamental human rights. Finally, the aspect of data protection as articulated under Article 8 of the ECHR imposes material limitations on the use of FRT by ensuring that individuals' personal data is handled with utmost care, transparency, and respect for their privacy rights. [149] The emphasis on informational self-determination and the necessity for a legitimate basis for data processing restricts arbitrary or invasive use of FRT, safeguarding individuals' rights to privacy and data protection. [150]

In terms of procedural limitations, Article 8 ECHR provides that the usage of intrusive measures like FRT require a high level of justification, demonstrating necessity in a democratic society. [151] This was emphasized in *Glukhin v. Russia*, where live FRT was deemed not necessary for a minor offense. Second, Article 8 ECHR also provides that there should be effective criminal or civil laws that must prohibit non-consensual filming and ensure thorough investigations, as seen in *Söderman v. Sweden*[152] and *Khadija Ismayilova v. Azerbaijan.*[153]

Finally, there are different aspects of the right to privacy that are governed by Article 8 of the ECHR. These provisions showcase a considerable overlap, with Article 7 of the

[146] See *Lozovyye v. Russia* (n 131) para 36.
[147] See *Khadija Ismayilova v. Azerbaijan* (n 132) para 139.
[148] See *López Ribalda and Others v. Spain* (n 136) paras 87–91.
[149] See *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (n 138) paras 133–134; *L.b. v. Hungary* (n 138) 103–104.
[150] See *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (n 138) paras 133–134; *L.b. v. Hungary* (n 138) 103–104.
[151] See *Glukhin v. Russia* (n 135) para 86.
[152] See *Söderman v. Sweden* (n 141) paras 40, 105.
[153] See *Khadija Ismayilova v. Azerbaijan* (n 132) para 112.

CFR designated as a "corresponding provision" for Article 8 of the ECHR, indicating identical content and scope.[154]

4.3.2 Article 7 of the CFR and Relevant Case Law on Video Surveillance and/or Facial Recognition

Article 7 of the CFR provides for the right to respect for private and family life, home, and communications. It prohibits arbitrary interference by public authorities into individuals' privacy without lawful justification.[155] On the same line, Article 8 of the ECHR safeguards the right to respect for private and family life, home, and correspondence, subject to certain limitations that are prescribed by law and necessary in a democratic society.[156]

In *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, the CJEU ruled that national laws allowing video surveillance in buildings for safety and property protection without data subject consent comply with EU law if they meet conditions under the EU's data protection law (Art. 6(1) lit. c) and Art. 7 lit. f) Directive 95/46, and Arts. 7, 8, 52 of the Charter).[157] This question was brought up by the Romanian Court which oversaw addressing a complaint by an apartment owner against the building's video surveillance system, arguing it violated EU data protection laws. The CJEU outlined three conditions for lawful video surveillance processing personal data: legitimate interest, purpose and necessity and balance of rights.[158]

First, it is stablished that the data controller must have a legitimate interest, such as protecting property, health, and life, especially if incidents like theft or vandalism have occurred.[159] Second, the processing of personal must serve the legitimate interest, and no less restrictive means should achieve the same result. The processing must follow the "data minimisation principle." In this case, previous security measures like an

[154] See Di Federico Giacomo (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer Netherlands 2011) 4 <https://link.springer.com/10.1007/978-94-007-0156-4> accessed 5 May 2024.
[155] Charter of Fundamental Rights of the European Union [2010] OJ C83/2 [hereinafter: CFR] art 7.2.
[156] ECHR, art. 8.1.
[157] See *TK v Asociaţia de Proprietari bloc M5A-ScaraA* [2019] ECJ Case C-708/18 [61].
[158] ibid 40.
[159] ibid 42–45.

intercom system proved insufficient. It is also provided that the national court must ensure minimal data collection, such as limiting surveillance to night hours or blocking unnecessary areas.[160] Finally, the court must balance the data subject's rights against the legitimate interest. This involves:[161]

- Considering the severity of the data rights infringement, especially if data is from non-public sources.
- Assessing the sensitivity of the data and the number of people with access to it.
- Evaluating the data subject's reasonable expectations regarding data processing.

At this point it is relevant to mention that Article 7 of the CFR addresses the right to private life and privacy, while Article 8 of the CFR focuses specifically on data protection. Although there is an overlap between privacy and data protection, the CFR treats them as distinct fundamental rights. This differs from Article 8 of the ECHR, where ECtHR case law has interpreted the right to private life to include data protection rights as well.[162]

Based on the information previously presented, there are various legal limitations on the use of Facial Recognition Technology (FRT) under Article 7 CFR. In terms of material limitations on the use of FRTs, first, FRT could be use if only while public authorities don't use it as an arbitrary interference without lawful justification.[163]

On the other hand, in terms of procedural limitations, as seen in the *TK v Asociaţia de Proprietari bloc M5A-ScaraA* case, video surveillance and, specifically the processing of personal data gathered through these technologies, must follow the conditions of legitimate interest, necessity, and balance of rights. Otherwise, their usage cannot be considered lawful. Additionally, we can conclude that Courts must balance data subjects' rights against legitimate interests, considering the severity of data rights infringement, sensitivity of data, and the data subject's reasonable expectations.

[160] ibid 46–51.
[161] ibid 52–60.
[162] See *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (n 138) paras 133–134; *L.b. v. Hungary* (n 138) 103–104.
[163] CFR, art 7.2.

4.3.3 Article 8 of the CFR and Relevant Case Law on Video Surveillance and/or Facial Recognition

Article 8 of the CFR stablishes that everyone has the right to the protection of personal data concerning them and that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.[164]

The Charter allows restrictions on the right to privacy, provided they comply with its provisions and those of the ECHR,[165] the prime example can be found in Article 8 of the CFR that explicitly addresses the protection of personal data, emphasizing fair processing and consent requirements. The introduction of this article was mainly product of the increasing importance of data protection because of the large-scale data collection and processing in databases.[166]

In *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, from 2014, the CJEU solved the question of validity that an Irish NGO did on the Data Retention Directive in the Digital Rights.[167] This Directive required providers of electronic communication services to store traffic and location data of users and granted national law enforcement authorities access to such data for investigating, identifying, and prosecuting serious crimes. The NGO argued that these obligations violated users' rights to privacy and data protection as outlined in Article 7 and 8 of the CFR.[168]

The CJEU ruled that both the data retention obligation and access rights breached privacy and personal data protection rights, concluding that the Directive is invalid.[169] While the Court acknowledged that combating terrorism and serious crimes is an

[164] ibid 8.
[165] See Pete Fussey and Daragh Murray, '"Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology"' (University of Essex Human Rights Centre 2019) 34.
[166] See 'Article 8 - Protection of Personal Data' (*European Union Agency for Fundamental Rights*, 25 April 2015) <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data> accessed 26 June 2024.
[167] See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECJ Joined Cases C-293/12 and C-594/12 [17].
[168] ibid 18.
[169] ibid 29, 71.

objective of general interest under Article 52(1) CFR, it emphasized that this objective alone does not justify the necessity of the data retention obligation.[170]

Based on the previous information gather, one can identify that in terms of material limitations on the use of FRTs, it is provided that personal data must be processed fairly for specified purposes, based on consent or another legitimate basis laid down by law.[171] Second, Article 8 also provides that individuals must have the right to access data collected about them and to have it rectified, so the data collected by FRT must be accessible and rectifiable for individuals.[172]

Now, in terms or procedural limitations on the use of FRTs, any data retention or processing must be necessary and proportionate, with a clear objective of general interest.[173]

4.4 Conclusion

In conclusion, there is a relationship between privacy rights and the use of facial recognition technologies under the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFR). First, it was concluded that privacy can be defined as a multifaceted right encompassing individual autonomy, data control, and protection from unwarranted surveillance.

Second, Article 8 of the ECHR and Article 7 of the CFR safeguard against arbitrary interference by public authorities and impose positive obligations on states to protect private life. The European Court of Human Rights (ECtHR) has ruled that video surveillance and facial recognition technologies, particularly when intrusive, require strong justification, as seen in cases like *Glukhin v. Russia* where the need for stringent criteria to justify the use of FRTs was highlighted. Furthermore, it is clear that Article 8 of the CFR specifically addresses data protection, emphasizing fair processing and

[170] ibid 42, 51.
[171] CFR, art 8.2.
[172] See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (n 167) para 17.
[173] ibid 42, 51.

consent as seen in the case *Digital Rights Ireland Ltd v Minister for Communications and others*.

Finally, it is necessary to mention that the impact of privacy rights on video surveillance and facial recognition technologies is significant. These technologies must meet strict legal standards to ensure they do not violate the right to privacy. Which is why, the evolving jurisprudence of the ECtHR and CJEU continues to uphold the balance between technological advancements and the right to privacy.

Chapter 5: Applicable Legal framework to FRT and AVS Regulatory Frameworks and Legal Considerations

5.1 Introduction

The deployment of FRTs and AVS by law enforcement authorities for mass surveillance purposes can bring up many tensions with the right to privacy and some EU regulations such as the GDPR, the LED and the AI Act. Even though these regulations were not created with the purpose of specifically regulating neither FRT neither AVS, these tools have nowadays become possible instruments to keep on check the use of FRT and AVS. After addressing in the last chapter, the right to privacy and its possible tensions with FRT and video surveillance, in this Chapter I will focus on presenting and the applicable legal framework applicable to FRT and possibly AVS.

5.2 Key Provisions in the General Data Protection Regulation

First, the General Data Protection Regulation (GDPR) is part of the EU legal framework on privacy and data protection, adopted in 2016 but it didn't enter into force until May 25th 2018. In the context of the usage of FRTs and AVS the GDPR becomes relevant due to the type of data that is handled by those systems. First, in its Recital 51, the GDPR provides that the processing of photographs should not systematically be considered as processing of special categories of personal data, as they are covered by the definition of biometric data only when processed through a specific technical means

allowing the unique identification or authentication of a natural person.[174] Due to the to the collection of facial features, this biometric data constitutes 'special categories of personal data'. It is relevant to mention that biometric data is part of the personal data category and due to this, the GDPR imposes strict criteria and limitations on the use of FRT, as it involves the processing of biometric data, which is sensitive and presents an increased risk to the privacy rights of individuals.[175] Specifically, Article 57 of the GDPR require the prior opinion of the national data protection supervisory authority for any measure restricting the protection of personal data.[176]

On the other hand, even though the text of the GDPR does not specifically mention data collected by AVS, it does discuss the processing of personal data, including sensitive data, and the rights of data subjects in relation to the collection and use of their personal information.[177] The term 'personal data is defined as any information related to an identified or identifiable natural person (referred to as the 'data subject'). An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.[178] However, as it was mentioned earlier, he AVS software used for the Paris Olympic Games doesn't collect or process any personal data, in principle.

Based on the GDPR provisions one can identify certain limitations for the usage of FRTs. In terms of material limitations on the usage of FRTs, these systems process biometric data (which is prohibited by the Olympic Law), and this falls under a special category of personal data, according to Recital 51 of the GDPR.[179] Due to this, the data

[174] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Recital 51.
[175] See Kouroupis (n 7) 146.
[176] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art 57.1(c).
[177] ibid 11.
[178] ibid 4.1.
[179] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

collected through FRTs must be subject to strict processing conditions, including the need for explicit consent or another lawful basis, adherence to principles of transparency, purpose limitation, data minimization, and security, as seen in Articles 5 and 6.[180] On a similar note, the GDPR's category of personal data, including that from FRTs, falls under GDPR if it can identify individuals directly or indirectly.[181] It is also relevant to mention that the GDPR provides that the processing of data requires clear communication and, often, explicit consent, especially for sensitive data as seen in Article 22 GDPR.[182]

However, Article 22 provides that individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions have legal effects or significantly affect them.[183] Exceptions to this right include cases where the decision is necessary for a contract, authorized by law with safeguards for the individual's rights, or based on explicit consent.[184] In these exceptions, appropriate measures must be taken to protect the individual's rights, including the right to human intervention, to express their viewpoint, and to contest the decision.[185]

Any decision involving special categories of personal data require additional safeguards unless specific conditions apply. [186] In the case of France using of AVS, it could be argued that since the conditions of deployments of this technology are compliant with Article 22 of the GDPR since the Olympic Law states that use of this technology will not replace human controllers.[187]

On the other hand, in terms of procedural limitations, the GDPR states that prior opinion from national data protection authorities is required for measures that restrict data

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Recital 51.
[180] ibid 5 and 6.
[181] ibid 4.1.
[182] ibid 22.4.
[183] ibid 22.
[184] ibid 22.2.
[185] ibid 22.3.
[186] ibid.
[187] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 10.4, 10.7.

protection.[188] Additionally, another limitation is that data subjects must be informed about data processing activities, and robust security measures must protect the data from unauthorized access.[189] The final limitation is related to the use of FRT for automated decision-making, and it provides that individuals have the right to contest automated decisions, including those derived from FRT specific exceptions apply.[190]

5.3 Key Provisions in the Law Enforcement Directive

When FRTs are used by law enforcement authorities, they also must be compliant with the LED according to the scope of the directive.[191] In the context of the usage of Facial Recognition Technology (FRT), the LED text does not specifically mention FRTs, but it does discuss the processing of biometric data to uniquely identify a person, which could potentially include facial recognition technology. This type of data processing is highlighted as posing a high risk to the rights and freedoms of data subjects, and appropriate technical and organizational measures are required to ensure compliance with data protection principles.[192]

Law enforcement authorities must ensure that the processing of biometric data, such as facial images, is necessary and proportionate to the objectives pursued.[193] Furthermore, Article 10 more specifically provides that when processing biometric data for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: where is authorised by Union or Member State law; or to protect the vital interests of the data subject or of another natural person; or where such processing relates to data which are manifestly made public by the data subject.[194]

---

[188] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art 36.1.
[189] ibid Recital 39.
[190] ibid 15.1(h).
[191] See Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016 art 2.
[192] ibid Recital 51.
[193] See Directive (EU) 2016/680 of the European Parliament and of The Council of 27 April 2016 art 4.1(b).
[194] ibid 10.

In relation with the use of AVS, the LED text does not explicitly mention video surveillance. However, it does discuss the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses, as well as the protection of public security and national security.[195] This could potentially encompass the use of video surveillance as a means of gathering and processing personal data for law enforcement and security purposes.

The processing of personal data in the context of law enforcement and borders is regulated by Directive 2016/680, (Law Enforcement Directive, LED). The LED deals with the processing of personal data by data controllers for 'law enforcement purposes' – which falls outside of the scope of the GDPR. Both the LED and the GDPR apply to the automated processing of personal data as well as manual processing within a filing system, as stated in Article 2(1) of the GDPR and Article 2 of the LED.[196] However, the LED serves as a more specialized framework compared to the GDPR (lex specialis), when public authorities are involved in processing personal data for preventing, investigating, detecting, or prosecuting criminal offences (Recitals 11 and 12 of the LED and Recital 19 of the GDPR)[197]. In accordance with the core legal principles of data protection outlined in Article 5 of the GDPR and Article 4 of the LED, the processing of facial images must meet the following criteria:

- Lawfulness, fairness, and transparency
- Specific, explicit, and legitimate purpose, as clearly defined by Member State or Union law
- Compliance with requirements concerning data minimization, accuracy, storage limitation, security, and accountability

Additionally, the LED Recital 51, provides that the controller should evaluate the likelihood and severity of the risk to the rights and freedoms of data subjects based on an objective assessment. Specific safeguards should be implemented to protect

[195] ibid 1.1.
[196] See European Parliament. Directorate General for Parliamentary Research Services. (n 5) 10.
[197] ibid.

vulnerable natural persons, such as children, and measures should be taken to prevent physical, material, or non-material damage resulting from data processing.[198]

To ensure compliance with the LED directive, appropriate technical and organizational measures must be implemented.[199] This includes adhering to data protection principles by design and by default, adopting internal policies, and conducting data protection impact assessments.[200] Furthermore, Member States may introduce legislative measures to restrict the data subject's right to access personal data, provided these measures are necessary and proportionate in a democratic society, considering the fundamental rights and legitimate interests of the data subject.[201]

Moreover, Member States should establish time limits for the erasure of personal data or periodic reviews of its storage necessity, with procedural measures to ensure adherence to these time limits.[202] Additionally, data controllers must clearly distinguish between personal data of different categories of data subjects, such as suspects, convicted individuals, victims, and others involved in criminal offenses.[203]

In terms of material limitations on the usage of FRTs under the LED, the processing of biometric data by law enforcement authorities must be necessary and proportionate in accordance with Article 10 LED, and this processing is allowed only when authorized by law, to protect vital interests, or if the data is public.[204]

Meanwhile, in terms of procedural limitations, it is stated in the LED that Law enforcement authorities must implement appropriate safeguards and conduct data protection impact assessments.[205] On a related note, personal data processing, acquired by FRT, must adhere to principles of data minimization, accuracy, and storage limitation as seen in Article 5 LED.[206] Finally, the LED also stablishes as a limitation

[198] See Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016 Recital 51.
[199] ibid 19.
[200] ibid 27.
[201] ibid 15.
[202] ibid 5.
[203] ibid 6.
[204] ibid 10.
[205] ibid 27.
[206] ibid 5.

that controllers must distinguish between different categories of data subjects, such as suspects or victims when deploying technologies that can identify individuals, like FRTs.[207]

5.4 Key Provisions in the Artificial Intelligence Act

The Artificial Intelligence Act (AI Act) is a new EU regulatory framework for AI systems, so that these systems are used in a safe, transparent[208], traceable, non-discriminatory and environmentally friendly way. The AI Act aims to establish a comprehensive regulatory framework for AI technologies, including FRT and AVS systems, by defining requirements for transparency, accountability,[209] and human oversight[210].

In terms of facial recognition technologies, Article 5 already establishes that the marketing, deployment, or utilization of AI systems aimed at creating or expanding facial recognition databases by indiscriminately scraping facial images from the internet or CCTV footage is prohibited.[211] Such practices exacerbate concerns regarding mass surveillance and may result in severe violations of fundamental rights, notably the right to privacy.[212] Furthermore, the same article provides that it is also prohibited the marketing, deployment, or utilization, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement.[213]

It is also relevant to mention that Recital 17 provides that 'remote biometric identification system' is defined as an AI system designed to identify individuals

[207] ibid 6.
[208] See Artificial Intelligence Act, Recital 53.
[209] ibid Recital 27.
[210] ibid Recital 1.
[211] ibid 5.1(e).
[212] ibid Recital 43.
[213] ibid 5.1(g).

without their active involvement, typically from a distance, by comparing their biometric data with data in a reference database.[214] These systems can identify multiple people or their behaviour simultaneously without their participation, but this excludes AI systems for biometric verification, which are used solely for authentication purposes, such as accessing services, unlocking devices, or securing premises, as they have a minor impact on fundamental rights. [215] The AI Act aims to prevent circumventing rules on real-time AI systems by imposing minor delays. [216] 'Real-time' systems capture, compare, and identify biometric data instantaneously or with minimal delay, using live or near-live material like video footage from cameras. In contrast, 'post' systems use pre-captured biometric data, comparing and identifying after a significant delay, with materials like CCTV footage. [217]

Under the same line, the AI Act also emphasizes that post-remote biometric identification systems, due to their intrusive nature, should have safeguards, in compliance with Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680.[218] Additionally, Article 3(34) reinforces that the term 'biometric data' includes personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, such as facial images.[219]

Recital 95 provides that these systems must be used proportionately, legitimately, and only when strictly necessary, targeting specific individuals, locations, and times, and based on a closed set of legally acquired video footage. They should never be used for indiscriminate surveillance in law enforcement and the conditions for their use must not circumvent the prohibition and strict exceptions for real-time remote biometric identification.[220]

Furthermore, Recital 125 provides that due to the complexity and risks of high-risk AI systems, a conformity assessment procedure involving third-party notified bodies is

[214] ibid Recital 17.
[215] ibid.
[216] ibid.
[217] ibid.
[218] ibid Recital 95.
[219] ibid 3.34.
[220] ibid Recital 95.

necessary. However, given current certifiers' experience and the different risks, third-party assessments should initially be limited. Generally, providers should conduct conformity assessments themselves, except for AI systems intended for biometric use.[221] Additionally, Recital 159 states that each market surveillance authority for high-risk AI systems in biometrics, as listed in the Regulation's annex, should have effective investigative and corrective powers, including access to all personal data and necessary information, particularly for law enforcement, migration, asylum, border control, justice, and democratic processes.[222] These authorities must act independently, with no limitations on accessing sensitive data per Directive (EU) 2016/680. This Regulation should not restrict the powers of national data protection authorities.[223]

On a related note, Article 7 provides that The Commission can adopt delegated acts to amend Annex III by adding or modifying high-risk AI use-cases if the AI systems are intended for areas listed in Annex III and pose a risk to health, safety, or fundamental rights equivalent to existing high-risk systems.[224] The assessment criteria must include the AI system's purpose, usage extent, data nature, autonomy, past harm, potential harm, user dependence, power imbalance, outcome reversibility, and potential benefits.[225] Additionally, if a high-risk AI system no longer poses significant risks and removing it does not reduce overall protection, the Commission can also amend Annex III to remove such systems.[226]

At this point, it is relevant to mention that according to the AI Act, AVS systems used by law enforcement authorities in Paris might or not be categorized as high-risk AI systems depending on whether they affect fundamental rights or not.[227] However, Article 5.1(h) states that AVS is considered prohibited if these systems use biometric data and are use in publicly accessible spaces by law enforcement authorities, unless they are used for preventing an specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable

[221] ibid Recital 125.
[222] ibid Recital 159.
[223] ibid.
[224] ibid 7.1.
[225] ibid 7.2.
[226] ibid 7.3.
[227] ibid 6.3.

threat of a terrorist attack.[228] This is relevant since Wintics have mention in different occasions that they AVS systems do not use biometric data and the text seems to emphasize that the high-risk characteristic, mainly depends on whether there is collection of biometric data.[229] Additionally, the text emphasizes the need for accuracy, reliability, and transparency in AI systems used in law enforcement to avoid adverse impacts, retain public trust, ensure accountability, and provide effective redress.

Furthermore, related to the use of FRTs and AVS, Article 86 provides that any person affected by a decision based on the output of a high-risk AI system listed in Annex III, except those under point 2, that has legal effects or significantly impacts their health, safety, or fundamental rights, has the right to obtain clear and meaningful explanations from the deployer about the AI system's role and the main elements of the decision.

There are various legal limitations on the use of Facial Recognition Technology (FRT) under the AI Act. In terms of material limitations, the use of AI systems, including FRT, for indiscriminate mass surveillance is prohibited according to Article 5.[230] Furthermore, the AI Act also stablishes that AI systems cannot categorize individuals based on sensitive biometric data, collected for example through FRTs, for inferring attributes like race or political beliefs.[231] Third, the Act distinguishes between real-time[232] and post-remote[233] biometric identification, emphasizing the greater intrusiveness of real-time systems.[234] Therefore, live FRT usage for the Olympic Games would have required a delicate balance and a justification for exercising a restriction on the right to privacy and other applicable provisions.

In terms of procedural limitations, the AI Act provides that high-risk AI systems require third-party conformity assessments to ensure compliance with safety, transparency, and accountability standards as seen in Recital 125. Additionally, Recital 95 provides that even non-real-time systems must comply with stringent safeguards under Union law.[235]

[228] ibid 5.1(h).
[229] ibid.
[230] ibid 5.1(e).
[231] ibid Recital 30.
[232] ibid 3.42.
[233] ibid 3.43.
[234] ibid Recital 39.
[235] ibid Recital 95.

5.5 Conclusion

Throughout this chapter, we have examined the intricate web of applicable legal frameworks, including the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and the emerging Artificial Intelligence Act (AI Act). First, it is clear that the GDPR imposes stringent requirements on the processing of biometric data, classifying it as a special category of personal data due to its sensitive nature. Law enforcement authorities utilizing FRT must navigate these regulations to ensure compliance, particularly regarding transparency, consent, and the minimization of data processing.

Second, the LED further sharpens the focus on the lawful and proportionate use of biometric data by law enforcement agencies. It provides that the processing of data must be strictly necessary and subject to appropriate safeguards, particularly when it involves sensitive personal data. This directive provides a specialized framework that complements the GDPR, addressing the specific contexts and risks associated with data processing for law enforcement purposes. The emphasis on data protection principles such as lawfulness, fairness, transparency, and the need for data minimization, accuracy, and security is crucial in maintaining the delicate balance between public safety and individual rights.

Finally, the AI Act introduces an additional layer of regulation, aimed at ensuring the safe, transparent, and accountable use of AI systems, including FRT and AVS. The AI Act provides stringent conditions under which these technologies can be deployed, particularly highlighting the prohibition of their use for mass surveillance purposes. It also emphasizes the need for a conformity assessment procedure to evaluate the compliance of high-risk AI systems, ensuring that they meet the necessary standards for accuracy, reliability, and transparency.

Chapter 6: Legal Limitations on Algorithmic Video Surveillance Technologies

6.1 Introduction

After discussing in previous chapters, the main differences between FRTs and AVS, and after presenting the relevant provisions in relation to the right to privacy and the GDPR, LED and the AI Act, it is relevant to explicitly mention and analyse the legal limitations on the use of FRTs and if all these limitations also apply for the use of AVS. Therefore, this chapter aims to analyse the legal restrictions that apply to AVS and technologies under Articles 8 ECHR, Article 7 CFR, the GDPR, the LED, and the AI Act, and whether these restrictions should be extended to the proposed use of AVS during the Olympic Games.

6.2 AVS usage for the Paris Olympic Games

After presenting the key limitations on the use of FRTs it is now necessary to analyse if these limitations are the same limitation on the use of AVS. As it was already mentioned in the introduction of this thesis, FRT is a type of AVS.[236] However, they are not the same and for this investigation the usage of these terms is not interchangeable between them, since when referring to AVS I am referring to all algorithmic video surveillance systems, except for FRTs. But even though both technologies are different, both can pose a risk to the right to privacy and certain legal frameworks such as the GDPR, LED and the AI Act. However, in the case of the Olympic Games in Paris 2024, only FRTs usage was prohibited stating it violates the right to privacy while the rest of AVS is allowed for use, only if it doesn't collect any type of biometric data.[237] This is why, after analysing the differences between both technologies and the limitations on the usage of FRT found in the relevant legal framework, I proceed to analyse if those limitation could also apply to AVS.

First, AVS in the Olympic Games of Paris claims it will not collect biometric data. [238] AVS identifies and recognizes silhouettes, but also assures that it does not store "neither images nor videos". [239] The JO law, particularly Article 7, expands this software's

[236] See Tripathy and Singh (n 8) 1.
[237] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 10.4.
[238] ibid.
[239] Gamaury (n 73).

capabilities to send real-time alerts to security operators when predefined thresholds are exceeded for eight types of events[240]:

- Failure to respect the direction of traffic
- Crossing a prohibited area
- The presence or use of a weapon
- An outbreak of fire
- A crowd movement
- One person on the ground
- Too much density
- An abandoned package[241]

Taking this into account, AVS in the Paris Olympic Games of 2024 will be understood as software that is not able to have any information relating to an identified or identifiable natural person, because it doesn't collect any personal data[242]. Due to the less intrusive nature of AVS, the limitations that could apply might be less compared to the ones that apply to FRTs. Some of the limitations outlined for FRT under Article 8 ECHR, Article 7 CFR, and Article 8 CFR might apply to Automated Video Surveillance (AVS) due to the following reasons.

6.3 Limitations applicable to AVS under ECHR and CFR

6.3.1 Limitations of AVS usage under Article 8 ECHR

First, in terms of Article 8 ECHR the limitation consisting of the protection against arbitrary interference by public authorities applies to AVS, ensuring that the surveillance system must be used judiciously, avoiding arbitrary monitoring that could infringe on individuals' private lives, for example: secretly collecting data of physical characteristics of individuals that go to a certain specific church.[243] Second, the positive obligation that States have to enact laws preventing non-consensual surveillance and

[240] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) art 7.
[241] Gamaury (n 73).
[242] See Khalifa and others (n 83) 329.
[243] ECHR, art. 8.

ensuring that AVS is used in a manner that respects individuals' private lives.[244] This includes avoiding unnecessary or excessive monitoring and ensuring that AVS does not become overly intrusive. Third, while AVS claims not to collect biometric data, it still must be used with consideration for its potential psychological and social impact on individuals.[245] The broad scope of "private life" under Article 8 ECHR implies that even non-biometric surveillance should be conducted in a manner that respects individual autonomy and identity.

In terms of procedural limitations, the use of AVS requires a high level of justification, demonstrating necessity in a democratic society. [246] This means AVS should be used only when necessary for legitimate purposes, such as public safety during the Olympic Games. Additionally, there must be effective legal frameworks prohibiting non-consensual filming and ensuring thorough investigations into any misuse of AVS.[247]

6.3.2 Limitations of AVS usage under Article 7 CFR

First, in terms of material limitations, AVS must be used with lawful justification, avoiding arbitrary interference, according to Article 7 CFR.[248] This principle requires that AVS is implemented for legitimate purposes and in a manner that does not unjustifiably infringe on privacy rights.

Now, in terms of procedural limitations, as seen in the case of video surveillance discussed in *TK v Asociaţia de Proprietari bloc M5A-ScaraA,* AVS must process data based on legitimate interest, necessity, and a balance of rights. [249] This means AVS should be justified by a legitimate interest (e.g., public safety), be necessary for achieving that interest, and not disproportionately infringe on individuals' rights. Finally, as it was discussed on the context of FRTs, the use of AVS Courts must balance the rights of individuals against the legitimate interests of public authorities, considering the severity of potential data rights infringements, the sensitivity of any

[244] See *Lozovyye v. Russia* (n 131) para 36.
[245] See *Khadija Ismayilova v. Azerbaijan* (n 132) para 139.
[246] See *Glukhin v. Russia* (n 135) para 86.
[247] See *López Ribalda and Others v. Spain* (n 136) paras 87–91.
[248] Charter of Fundamental Rights of the European Union [2010] OJ C83/2 [hereinafter: CFR] art 7.2.
[249] See *TK v Asociația de Proprietari bloc M5A-ScaraA* (n 157) para 40.

incidental data, and the reasonable expectations of individuals regarding surveillance.[250]

6.3.3 Limitations of AVS usage under Article 8 CFR

While AVS does not collect biometric data nor personal data and is less intrusive than FRTs, it is still subject to certain limitations under Article 8 of the CFR. In terms of material limitations, even though AVS claims not to collect biometric data nor personal data, any incidental data must be processed fairly and for specified purposes. This means any minimal data that might be collected must be handled with a clear, lawful purpose.[251] Finally, in terms of procedural limitations, any data processing by AVS must be necessary and proportionate, with a clear objective of general interest.[252] This means the use of AVS should be justified by a legitimate public interest and should not exceed what is necessary to achieve that interest.

6.4 Limitations applicable to AVS under the GDPR, the LED and the AI Act

6.4.1 Limitations of AVS usage under the GDPR

While AVS does not collect biometric data nor personal data and is less intrusive than FRTs, it is still subject to certain limitations under the GDPR. Even though AVS claims not to collect biometric data nor personal data, there is a chance it will collect this by accident. Therefore, incidental data must be processed fairly and for specified purposes. AVS systems must comply with GDPR when processing personal data, even if it is not explicitly biometric. This includes obligations for transparency, consent, and security as analysed in Chapter 5.2.[253] However, in the Paris Olympic Games, since it is already stated that AVS will not collect any biometric data nor personal data (not even

[250] ibid 52–60.
[251] Charter of Fundamental Rights of the European Union art 8.
[252] See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (n 167) paras 42, 51.
[253] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) art 22.4.

accidentally) its use may fall outside of these stringent requirements illustrated in the GDPR. Therefore, the limitations on FRTs under the GDPR cannot be applied to AVS, due to the difference between both technologies.

6.4.2 Limitations of AVS usage under the LED

Due to the intrusive nature of AVS, when used by law enforcement, AVS must meet LED the principles of necessity, proportionality, and appropriate safeguards even if it does not collect and process personal data, this is because of the possibility of the AVS incidentally gathering personal data.[254] However, in the Paris Olympic Games, since it is already stated that AVS will not collect any biometric data nor personal data (let's assume that not even accidentally) its use may fall outside of these stringent requirements illustrated in the LED.

6.4.3 Limitation of AVS usage under the AI Act

As it was already mentioned, AVS may be classified as high-risk AI systems depending on their impact on fundamental rights.[255] If AVS involves biometric data, it is subject to strict limitations and prohibitions under the AI Act. requiring conformity assessments and compliance with safeguards. [256] However, in the case of the Olympic Games it has been already stablished that AVS does not collect/process biometric nor personal data.

Based on the provisions of the AI Act, the usage of AVS for the Olympic Games in Paris would be subject to certain legal limitations, both material and procedural. Some of the limitations are, for instance, the prohibition of real-time remote biometric identification of the AI Act.[257] If the AVS software collected accidentally any data to identify individuals, it would end up violating this measure. Second, as the AVS software is trained to recognize shadows and does not collect personal data, it would

[254] See Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016 art 4.
[255] See Artificial Intelligence Act art 7.2.
[256] ibid 5.1(h).
[257] ibid.

need to ensure that it does not inadvertently create or expand facial recognition databases through the collection of any type of image data due to this prohibition in the AI Act.[258] Third, and in relation with procedural limitation, deployers of AI systems that generate or manipulate image, audio, video, or text content are required to disclose that the content has been artificially generated or manipulated.[259] This obligation applies to the AVS software if it generates or manipulates any type of content.

6.5 Conclusion

The GDPR, LED, and AI Act collectively establish a comprehensive framework to govern the deployment of FRT and AVS technologies by law enforcement authorities in the EU. These regulations aim to strike a balance between leveraging technological advancements for public safety and protecting individuals' fundamental rights to privacy and data protection. However, it can be concluded that not all the legal limitations that apply to the use of FRTs can be applied on the use of AVS, especially since these systems don't process biometric nor personal data. Finally, the compliance of AVS with the framework mentioned requires careful consideration of legal requirements, including obtaining lawful bases for processing sensitive data, implementing appropriate safeguards, and ensuring transparency and accountability in the use of surveillance technologies. Even though the AVS does not represent the same level of risk as FRTs toward the right to privacy, this does not mean that the AVS usage does not pose any risk in terms of the right to privacy. This chapter perfectly illustrates that further regulation and research in the field of AVS is required, since this is typically limited to FRTs.

CONCLUSION

The aim of this thesis was to determine whether FRT limitations could also be applied to the use of AVS in order to protect the right to privacy of individuals, in the scenario of the Paris Olympic Games. In line with this aim, the research question was formulated

[258] ibid 5.1(e).
[259] ibid 50.4.

as: *'Are the legal limitations on Facial Recognition Technologies under Articles 8 ECHR, Article 7 CFR, the GDPR, the LED, and the AI Act, equally applicable to Algorithmic Video Surveillance systems used during the 2024 Paris Olympic Games?'*

This research conducted in this thesis has provided a comprehensive analysis of the legal restrictions that apply to Facial Recognition Technologies (FRT) under Articles 8 ECHR, Article 7 CFR, the GDPR, the LED, and the AI Act.

The fundamental characteristics of FRT and AVS technologies proposed for the Olympic Games were thoroughly examined, highlighting the differences between the two technologies in terms of their level of intrusiveness and the type of data they collect and process. The Olympic Law's stance on the deployment of AVS and the prohibition of FRTs was also explored. This allowed to shed light on the legal limitations concerning the use of FRT and AVS in public spaces, based on the right to private life as protected under Article 8 ECHR and Articles 7 and 8 CFR. Additionally, I managed to present and analyse the legal limitations concerning the use of FRT and AVS on the basis of the GDPR, LED, and the new AI Act.

Based on this comprehensive analysis, it can be concluded that the legal restrictions that apply to FRT, at least some of them, under the legal frameworks could also be applicable to AVS technologies being deployed during the 2024 Paris Olympic Games. Through this research I have been able to highlight the potential risks to privacy and data protection posed by both FRT and AVS technologies, and the need for explicit legal limitations and safeguards to ensure the protection of fundamental rights in the context of mass surveillance. Even though the AVS does not represent the same level of risk as FRTs towards the right to privacy, this does not mean that the AVS usage does not pose any risks.

As a final thought I would like to add that, in the context of the Paris Olympic Games, the prohibition of FRT does not provide a full protection of the right to privacy as the French Government might think. As it was discussed throughout this research, AVS can also be intrusive on the right to privacy. The use of either AVS or FRTs should be publicly discussed and openly described, in order for people to actually be informed and know what to expect about the deployment of these technologies. This will help to

also spot any misuse of the technology that can open the door for secret surveillance disguised as a malfunction or as a non-intrusive system. I have to highlight the effort of the French Government on prohibiting the use of FRTs, but it seems that they limited their understanding of "breach of the right to privacy" onto whether the technology collects biometric data/personal data. This assumption is incorrect as it has been illustrated by the ECtHR, that the right to privacy encapsulates a wide scope which includes personal image and so on.

Further regulation and research in the field of AVS is required, especially since all this research and regulation has been typically limited to FRTs. With the Olympic Games approaching soon, now it remains to see how AVS is used in the real day-to-day basis and hope that the system doesn't interfere secretly nor drastically with the right to privacy of individuals.

BIBLIOGRAPHY

- Adams J and Almahmoud H, 'The Meaning of Privacy in the Digital Era' (2023) 15 International Journal of Security and Privacy in Pervasive Computing (IJSPPC) 1

- 'AI in Video Surveillance | Isarsoft' (19 September 2023) <https://www.isarsoft.com/article/ai-in-video-surveillance> accessed 5 July 2024
- 'Article 8 - Protection of Personal Data' (*European Union Agency for Fundamental Rights*, 25 April 2015) <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data> accessed 26 June 2024

- Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial Recognition in Online and Mobile Services' <https://www.pdpjournals.com/docs/87997.pdf>

- Bowling B and Iyer S, 'Automated Policing: The Case of Body-Worn Video Special Issue on Law, Liberty and Technology: Criminal Justice in the Context of Smart Machines' (2019) 15 International Journal of Law in Context 140

- Brobst JA, 'The Metal Eye: Ethical Regulation of the State's Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement' (2018) 55 California Western Law Review 1

- Buolamwini J and others, 'Facial Recognition Technologies: A Primer' <https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf>

- Charpentier D, 'Paris 2024 : il y aura bien des caméras « intelligentes » pour les Jeux olympiques' (*leparisien.fr*, 23 March 2023) <https://www.leparisien.fr/jo-paris-2024/paris-2024-il-y-aura-bien-des-

cameras-intelligentes-pour-les-jeux-olympiques-23-03-2023-ZUGRDLKEXJDSVD6QGXKIKBYDTM.php> accessed 1 March 2024

- Cole MD, 'Recent Developments and Overview of the Country and Practitioner's Reports Reports: Introduction' (2020) 6 European Data Protection Law Review (EDPL) 94

- Directorate-General for Parliamentary Research Services (European Parliament), Madiega T and Mildebrath H, *Regulating Facial Recognition in the EU: In Depth Analysis* (Publications Office of the European Union 2021) <https://data.europa.eu/doi/10.2861/140928> accessed 26 February 2024

- Dubedout C, 'Nice "Safe City" : An Acceleration of Experiments for Three Years' (*MIAI*, 24 February 2020) <https://ai-regulation.com/safe-city-project-in-nice-testing-facial-recognition/> accessed 1 March 2024

- Efa G, 'Facial Recognition in European Cities - Read Our New Study' (*Greens/EFA*, 22 October 2021) <https://www.greens-efa.eu/opinions/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/> accessed 26 February 2024

- 'Ethics Guidelines for Trustworthy AI' <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>

- European Commission, 'WHITE PAPER On Artificial Intelligence - A European Approach to Excellence and Trust' <https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf>

- European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf>

- European Parliament. Directorate General for Parliamentary Research Services., *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues.* (Publications Office 2021) <https://data.europa.eu/doi/10.2861/91831> accessed 17 April 2024

- *Regulating Facial Recognition in the EU: In Depth Analysis.* (Publications Office 2021) <https://data.europa.eu/doi/10.2861/140928> accessed 27 November 2023
- 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (*European Union Agency for Fundamental Rights*, 21 November 2019) <http://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 26 February 2024

- Fussey P and Murray D, '"Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology"' (University of Essex Human Rights Centre 2019)

- Gamaury L, 'Aux JO, de la vidéosurveillance sans reconnaissance faciale, vraiment ?' (*www.20minutes.fr*, 4 March 2024) <https://www.20minutes.fr/sport/jo_2024/4077797-20240304-jo-paris-2024-videosurveillance-reconnaissance-faciale-vraiment> accessed 31 May 2024

- Gati B, 'Data Protection Aspects of the Use of Facial Recognition Systems for Law Enforcement Criminal Law Section' (2023) 2023 Collection of Papers from the Conference Organized on Occasion of the Day of the Faculty of Law 306

- Gerards J, *General Principles of the European Convention on Human Rights* (Second edition, Cambridge University Press 2023)

- Giacomo DF (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer Netherlands 2011) <https://link.springer.com/10.1007/978-94-007-0156-4> accessed 5 May 2024

- Hafiz Sheikh AA, ‘Facial Recognition Technology and Privacy Concerns’ (21 December 2022) <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns>
- ‘House of Lords - Surveillance: Citizens and the State - Constitution Committee’ <https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm> accessed 28 February 2024
- ‘JO 2024 Loi du 19 mai 2023 Jeux Olympiques et Paralympiques | vie-publique.fr’ <https://www.vie-publique.fr/loi/287639-jo-2024-loi-du-19-mai-2023-jeux-olympiques-et-paralympiques> accessed 31 May 2024

- ‘JO Paris 2024 : Comment l’intelligence Artificielle va Aider à Analyser Les Images de La Vidéosurveillance ? - France Bleu’ (*ici, par France Bleu et France 3*, 16 February 2024) <https://www.francebleu.fr/infos/societe/jo-paris-2024-comment-l-intelligence-artificielle-va-aider-a-analyser-les-images-de-la-videosurveillance-1423127> accessed 1 March 2024

- Kahn J, ‘Privacy as a Legal Principle of Identity Maintenance’ (2002) 33 Seton Hall Law Review 371

- Kaplina O and others, ‘Application of Artificial Intelligence Systems in Criminal Procedure: Key Areas, Basic Legal Principles and Problems of Correlation with Fundamental Human Rights’ (2023) 2023 Access to Justice in Eastern Europe 147

- Khalifa OO and others, ‘Video-Based Abnormal Behaviour Detection in Smart Surveillance Systems’ in Khalid Isa and others (eds), *Proceedings of the 12th National Technical Seminar on Unmanned System Technology 2020* (Springer 2022)

- Kouroupis K, ‘Facial Recognition: A Challenge for Europe or a Threat to Human Rights?’ (2021) 2021 European Journal of Privacy Law & Technologies

<https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1265> accessed 26 February 2024

- Lehr AK and Crumpler W, 'Facial Recognition and Human Rights Law' (Center for Strategic and International Studies (CSIS) 2021) <http://www.jstor.org/stable/resrep33749.8> accessed 27 November 2023

- Mekrani A, 'The Future of Facial Recognition in Relation to Privacy A Research on the Added Value of the Emerging Guidance of the European Union on the Use of Facial Recognition Technologies' (Tilburg Universiy 2020)

- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 'La Lettre de la DAJ – La loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions' (8 June 2023) <https://www.economie.gouv.fr/daj/la-lettre-de-la-daj-la-loi-relative-aux-jeux-olympiques-et-paralympiques-de-2024> accessed 21 June 2024

- Ministry News, 'Lancement de l'expérimentation « vidéo-intelligentes » en vue de la sécurisation des Jeux Olympiques | Ministère de l'Intérieur et des Outre-mer' (19 April 2024) <https://www.interieur.gouv.fr/actualites/actualites-du-ministere/lancement-de-lexperimentation-video-intelligentes-en-vue-de> accessed 31 May 2024

- Miyamoto I, 'Surveillance Technology Challenges Political Culture of Democratic States' (Daniel K Inouye Asia-Pacific Center for Security Studies 2020) <https://www.jstor.org/stable/resrep26667.9> accessed 27 November 2023

- O'Flaherty M, 'Facial Recognition Technology and Fundamental Rights Opinions' (2020) 6 European Data Protection Law Review (EDPL) 170

- Orwell G, *Nineteen Eighty-Four* (Bernard Crick ed, Clarendon Press [u.a] 1984)

- Packulak M, ‘Who Watches the Watchers: Oversight of State Surveillance’ (2022) 45 Manitoba Law Journal 101

- Roux K, ‘2024 Olympics: From Algorthmic Video Surveillance to Facial Recognition, There is Only One Step’ (26 April 2024) <https://www.amnesty.fr/liberte-d-expression/actualites/jo-paris-de-la-videosurveillance-algorithmique-a-la-reconnaissance-faciale-il-n-y-a-qu-un-pas#:~:text=La%20reconnaissance%20faciale%20ne%20sera,ont%20m%C3%AAme%20%C3%A9rig%C3%A9%20en%20principe.>

- Semivolos A, ‘The Advent of Facial Recognition and the Erosion of the Rule of Law in “Moscow Smart City”’ (2022) 29 Cardozo Journal of Equal Rights and Social Justice 345

- Sénat, ‘Séance du 24 janvier 2023’ (2023) <https://www.senat.fr/seances/s202301/s20230124/s20230124011.html#Niv1_SOM9> accessed 22 June 2024

- Solarova S and others, ‘Reconsidering the Regulation of Facial Recognition in Public Spaces’ (2023) 3 AI and Ethics 625

- Surette R, ‘The Thinking Eye - Pros and Cons of Second Generation CCTV Surveillance Systems’ (2005) 28 Policing: An International Journal of Police Strategies and Management 152

- Tripathy A and Singh V, ‘AI-Powered CCTV Cameras Are the Future of Security and Surveillance, How Presear Softwares Deliver Advanced CCTV Video Analytics Softwares as a Hybrid Software Package Minimizing Your Cost’ (Zenodo 2022) <https://zenodo.org/records/6570013> accessed 30 May 2024

- Turgut Bilgic E, ‘Personal Data Protection in the Context of Video Surveillance in Public Areas: The Case of France’ (2023) 13 Hacettepe Hukuk Fakultesi Dergisi 414

Case Law

- *Antović and Mirković v Montenegro* [2017] ECtHR 70838/13
- *Bărbulescu v Romania* [2017] ECtHR [GC] 61496/08
- *Décision n° 2023-850 DC du 17 mai 2023 | Conseil Constitutionnel* [2023] Conseil Constitutionnel 2023-850
- *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECJ Joined Cases C-293/12 and C-594/12
- *Drelon v France* [2022] ECtHR 3153/16, 27758/18
- *Glukhin v Russia* [2023] ECtHR 11519/20
- *Khadija Ismayilova v Azerbaijan* [2019] ECtHR 65286/13, 57270/14
- *Kroon and Others v the Netherlands* [1994] ECtHR 19016/18, 56976/18, 41405/21, 56248/21, 56279/21, 57904/21, 61341/21, 12360/22, 30061/22, 38307/23
- *L.b v Hungary* [2023] ECtHR [GC] 36345/16
- *Libert v France* [2018] ECtHR 588/13
- *López Ribalda and Others v Spain* [2019] ECtHR [GC] 1874/13, 8567/13
- *Lozovyye v Russia* [2018] ECtHR 4587/09
- *Peck v the United Kingdom* [2003] ECtHR 60898/00
- *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECtHR [GC] 931/13
- *Smirnova v Russia* [2003] ECtHR 46133/99, 48183/99

- *Söderman v Sweden* [2013] ECtHR [GC] 5786/08

- *TK v Asociaţia de Proprietari bloc M5A-ScaraA* [2019] ECJ Case C-708/18

Legislation

- Artificial Intelligence Act 2024
- Charter of Fundamental Rights of the European Union 2012
- Directive (EU) 2016/680 of The European Parliament and of The Council of 27 April 2016 2016
- LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (1) 2023 (2023-380)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016