AI-Assisted Security at the Paris 2024 Olympic Games

Alexandre Lodie, Stephanie Celis Juarez

January27th, 2023

AI-REGULATION.COM

AI-Assisted Security at the Paris 2024 Olympic Games: From Facial Recognition to Smart Video

By Alexandre Lodie & Stephanie Celis Juarez

To cite this article:

A. Lodie, S. Celis Juarez, AI-Assisted Security at the Paris 2024 Olympic Games: From Facial Recognition to Smart Video, AI-Regulation.com, January 27th, 2023.

AI-Regulation.com

CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

AI-Assisted Security at the Paris 2024 Olympic Games:
From Facial Recognition to Smart Video

On November 23rd, 2022 an article by *Le Parisien*, a French Newspaper, revealed that the French Government had dropped its project to deploy facial recognition to support security arrangements at the 2024 Paris Olympics[1]. In fact, the debate on the possible implementation of facial recognition systems during the Olympic Games is part of a broader debate which divides political leaders on whether AI-driven biometric systems should be used to monitor public places.

Before digging into too much detail, it is worth recalling what facial recognition is. The 'Commission Nationale de l'Informatique et des Libertés' (CNIL, French data protection authority) defines this technology as "*a probabilistic software application that can automatically recognise a person based on its facial attributes in order to authenticate or identify them*"[2]. This technology consists of processing biometric data, which are data that enable the unique identification of a person[3]. In the case of facial recognition, a biometric template is extracted which identifies a person via the features of his/her face[4].

This technology can be used for two main functionalities - verification and identification (these functionalities can however be divided into sub-categories)[5]. The verification functionality basically "*involves (...) a 1-1 comparison, between a single captured facial image of a user (for instance taken at an eGate at the border) and the biometric photo stored in a biometric token (for instance a passport) or an index. Verification is most often considered as a synonym to "authentication*""[6].

On the other hand, identification techniques involve a comparison between a single facial image and a plurality of facial images contained in a database. These techniques are used for instance by law enforcement authorities in order to identify a suspect.

However, there are other kinds of AI-driven technology that can be used to analyse images. These systems are often described as "smart video devices" or "augmented cameras". The

[1] WESFREID (M.), "Paris 2024 : pas de reconnaissance faciale aux JO", Le Parisien, November 23rd, 2022, available at: https://www.leparisien.fr/politique/paris-2024-pas-de-reconnaissance-faciale-aux-jo-23-11-2022-4E3FP2XBWZC4LBY3B4UMPA3QPE.php?ts=1669200293918
[2] CNIL, "Facial Recognition: For a debate living up to the challenges", November 15th 2019, p.3, available at: https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf
[3] *Ibidem.*
[4] *Ibidem*.
[5] See CHRISTAKIS (T.), BANNELIER (K.), CASTELLUCCIA (C.), LE METAYER (D.), "Mapping the Use of Facial Recognition in Public Spaces in Europe - Part 2: Classification", Report of the AI-Regulation Chair (ai-regulation.com), MIAI, May 2022, available at: https://ai-regulation.com/wp-content/uploads/2022/05/Facial-Recognition-in-Europe-Part2.-Classification.pdf
[6] CHRISTAKIS (T.), BANNELIER (K.), CASTELLUCCIA (C.), LE METAYER (D.), "Mapping the Use of Facial Recognition in Public Spaces in Europe - Part 3: Facial Recognition for Authorisation Purposes", Report of the AI-Regulation Chair (ai-regulation.com), MIAI, May 2022, available at: https://ai-regulation.com/wp-content/uploads/2022/05/Report3-MAPFRE-Christakis-et-al.pdf

French DPA stated in a report that "*(t)his is a technology known as 'computer vision', which is one of the branches of 'artificial intelligence', consisting of equipping systems with digital image analysis capabilities, by extracting information such as pattern recognition, movement analysis, object detection*"[7].

Such AI-driven technology is increasingly being deployed for a wide variety of purposes, notably, to monitor sports venues. For instance, the Dutch Government funded a plan to implement smart video trials in three stadiums in the Netherlands in order to combat discrimination during Eredivisie football games. In particular, "a trial at Feyenoord's De Kuip stadium will use technology to identify the causes behind discriminatory behaviour, how to identify it, and how to nip it in the bud. The technology will also be able to determine the mood of other fans when in proximity to such discrimination"[8].

Despite this technology being implemented more and more in sports venues, there have been very few assessments on whether the deployment of the technology has been successful in providing effective security at events. In spite of the lack of information available, AI-driven systems are often perceived or presented as a silver bullet for ensuring the safety of major public events.

We will therefore consider why the facial recognition technology project aimed at ensuring the safety of the Paris Olympic Games was abandoned (I), despite the French government still considering smart video devices to be an appropriate solution (II).

I. The abandonment of the use of facial recognition for both identification and authentication purposes

Facial recognition techniques basically enable automated processing of facial images in order to identify or authenticate a person, which is why they have been used in major public events throughout the world, such as the Tokyo Olympic Games (for authentication purposes)[9] and the Football World cup held in Qatar. An article by Biometric Update claimed that the "*FIFA World Cup 2022 in Qatar will be held at 8 stadiums and watched by millions of fans, along with 15,000 CCTV cameras hooked up to facial recognition systems*"[10]. From this perspective facial recognition is perceived as a powerful security tool that enables law enforcement to monitor public places.

---

[7] CNIL, "Caméras dites "intelligentes" ou "augmentées" dans les espaces publics: Position sur les conditions de déploiement", July 2022, p. 5, available at: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf

[8] MCCASKILL (S.), "Dutch FA uses smart cameras and AI to tackle discrimination in venues", Sportspromedia, June 13th 2022, available at: https://www.sportspromedia.com/news/dutch-fa-knvb-ai-video-tech/

[9] See The Government of Japan, "All is Ready for a Safe and Secure Tokyo 2020 Games", Japan gov website, **https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html**

[10] BURT (C.), "Qatar equips 15,000 cameras with facial recognition for soccer World Cup 2022", Biometric Update, August 18th, 2022, available at: https://www.biometricupdate.com/202208/qatar-equips-15000-cameras-with-facial-recognition-for-soccer-world-cup-2022

It is perhaps easy to understand why French authorities were interested in the deployment of facial recognition to support security arrangements at the 2024 Paris Olympic Games. For instance, French Senator Claude Kern claimed, during a Senate hearing involving the French Minister of the Interior, Gérald Darmanin, that "*Violence in stadiums has become a constant concern, facial recognition tools are a tool; the Japanese ambassador explained to us how his country has deployed this tool and he advised us to do so for the Olympics: is France ready to deploy techniques that have proved their worth in Japan?*"[11].

This debate has become so prominent that the French Government was pressed to act following the incidents that took place during the UEFA champions league final in Paris, in which supporters without tickets succeeded in entering the stadium while other supporters with tickets were denied entry to the stadium[12]. Following these events, some French politicians claimed that facial recognition techniques could have been deployed to prevent such events, and that they should be deployed in future for major public events, including the 2024 Olympic Games. In particular, the Mayor of Nice, Christian Estrosi, advocated implementing such systems in the aftermath of the events that took place during the Champions League final[13]. It is not the first time that the Mayor of Nice has pleaded in favour of the deployment of facial recognition devices. Indeed, the Nice City Council had experimented with the deployment of facial recognition systems during the 2019 edition of the Nice Carnival[14].

However, facial recognition systems cover a wide array of systems deployed for different purposes[15]. It is thus important to see what systems the French authorities were considering to support security arrangements for the 2024 Paris Olympic games and why they eventually decided to abandon this project.

Parliamentary sources have shown that French lawmakers were considering adopting a legal framework to enable the deployment of two different facial recognition systems for two different purposes, including for the safety of major public events.

---

[11] Sécurité des jeux Olympiques et Paralympiques de 2024 - Audition de M. Gérald Darmanin, ministre de l'intérieur et des outre-mer, Commission des lois, October 25th, 2022, available at: https://www.senat.fr/compte-rendu-commissions/20221024/lois.html

[12] "Ligue des champions : les incidents en marge de la finale fustigés par la presse étrangère", Le Monde, May 29th, 2022, available at: https://www.lemonde.fr/sport/article/2022/05/29/honteux-scandale-la-presse-etrangere-deplore-les-incidents-en-marge-de-la-finale-de-la-ligue-des-champions_6128091_3242.html

[13] SENECHAL (J.), "La reconnaissance faciale serait-elle utile pour lutter contre la violence dans les stades ?", Le Figaro, June 2nd, 2022, available at: https://www.lefigaro.fr/actualite-france/la-reconnaissance-faciale-serait-elle-utile-pour-lutter-contre-la-violence-dans-les-stades-20220602?utm_medium=Social&utm_campaign=echobox&utm_source=Twitter&origine=VWT16001#Echobox=1654190841-1

[14] SERRIES (G.), "Mais comment Christian Estrosi pourra faire de l'IA sans reconnaissance faciale ?", zdnet, June 17th, 2022, available at: https://www.zdnet.fr/actualites/mais-comment-christian-estrosi-pourra-faire-de-l-ia-sans-reconnaissance-faciale-39943480.htm

[15] CHRISTAKIS (T.), BANNELIER (K.), CASTELLUCCIA (C.), LE METAYER (D.), "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification", Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

Although there is very little information available about how facial recognition was intended to be used for the Paris Olympics, it seems that the deployment of Biometric identification systems was considered. Indeed, a recent senatorial report reads as follows:

"*France will host two major sporting events in 2023 (Rugby World Cup) and 2024 (Olympic and Paralympic Games). Because of the major security challenges they pose, many stakeholders had advocated a national experiment sufficiently far in advance to be able to use real-time identification by facial recognition in the public space*"[16]

Besides, in this same report, French senators concluded that although the use of facial recognition for identification poses high risks to people's Human Rights, such a use could be authorised on an exceptional basis for certain major events. More specifically, they stated that *"(i)n particular, we believe that there should be a clear ban on biometric surveillance at public events and places of worship, but we can consider granting it in a number of cases where there may be a risk - the Olympics, for example"*[17].

On the other hand, the deployment of facial recognition for authorisation purposes was also considered. French secretary Cedric O stated in front of the Senate that "*(the decision not to deploy identification systems) should not prevent us from moving forward on the authentication of certain personnel for access to Olympic venues, for example*"[18].

In a similar vein, the Director of Public Liberties and Legal Affairs at the Ministry of the Interior claimed that the Minister of the Interior was considering *"the implementation of experiments designed to secure these events and the large gatherings they involve. However, from now on it should only be a question of access control devices for personnel or athletes, in line with the comments made by the Secretary of State for Digital Transition and Electronic Communications"*[19]. According to these statements, the facial recognition systems that were considered involved verification systems[20], i.e., systems that enable verification that the person is who they say they are, and which would not involve identification.

Even though there is no clear explanation about why the deployment of authentication techniques was seriously considered by the French executive branch, it is probably because such systems can be deployed in such a way as to involve people's consent, and they are programmed to capture delimited categories of people. With regard to this particular technology, French senators claimed that "*Authentication devices, which allow secure and fluid*

[16] DAUBRESSE (M-P.), DE BELENET (A.), DURAIN (J.), Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, Sénat, 10 mai 2022, p. 44.
[17] *Ibid*, p. 111.
[18] COMPTE RENDU DE L'AUDITION DE M. CÉDRIC O, SECRÉTAIRE D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES, *Mercredi 16 mars 2022*
[19] See DAUBRESSE (M-P.), DE BELENET (A.), DURAIN (J.), Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, Sénat, 10 mai 2022, p.45
[20] CHRISTAKIS (T.), BANNELIER (K.), CASTELLUCCIA (C.), LE METAYER (D.), "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

control of access, should be authorised when they are based on the consent of individuals. In certain very specific cases and on an experimental basis, they could also be made compulsory for access to areas requiring exceptional security"[21].

Eventually both authorisation and identification systems were abandoned as a means of supporting security arrangements for the Olympic games. Indeed, the French Minister of the Interior stated that "*the city of Paris has announced technological tools that the Parliament does not allow today. I have already expressed myself on this point: I am not in favour of facial recognition, a tool which is a societal choice and which entails a degree of risk - because I believe that we do not have the means to guarantee that this tool will not be used against citizens under another regime*"[22]. In spite of this clear position aimed at rejecting the deployment of facial recognition systems, some lawmakers are still pushing for the implementation of such systems[23]. In particular, as stated by the CNIL's Chair, a right-wing MP has introduced an amendment – which was eventually rejected – aiming at reintroducing facial recognition in the bill[24].

This rejection of the use of facial recognition is all the stronger when it comes to identification systems. From this perspective, French secretary Cedric O stated in front of the Senate that "*[t]he decision to use identification for the 2024 Olympic Games should have been taken by now: the Government chose not to do so, given the political context and the sensitivity of the subject. This therefore effectively prohibits the use of identification devices (...)"*[25].

As regards the sensitiveness of identification systems, there is a huge debate going on in Europe about whether such systems should be banned because of the risks they pose to fundamental rights. This issue is currently being discussed by the Council of the EU and the European parliament during the negotiations related to the adoption of the AI Act[26].

With regard to this issue, the European Data Protection Board (EDPB) called for a general ban on such techniques deployed in open spaces. The European privacy watchdog claimed that "*remote biometric identification of individuals in publicly accessible spaces poses a high risk*

---

[21] DAUBRESSE (M-P.), DE BELENET (A.), DURAIN (J.), Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, Sénat, 10 mai 2022, p. 113.

[22] Sécurité des jeux Olympiques et Paralympiques de 2024 - Audition de M. Gérald Darmanin, ministre de l'intérieur et des outre-mer, Commission des lois, October 25th, 2022, available at: https://www.senat.fr/compte-rendu-commissions/20221024/lois.html

[23] See KAYALI (L.), "France plots surveillance power grab for Paris 2024 Olympics", Politico, January 18th, 2023.

[24] See "JO 2024 : la Cnil appelle les parlementaires à ne pas introduire de la reconnaissance faciale dans la loi", Francetvinfo, January 24th, 2023, available at: https://www.francetvinfo.fr/internet/video-jo-2024-la-cnil-appelle-les-parlementaires-a-ne-pas-introduire-de-la-reconnaissance-faciale-dans-la-loi_5620073.html

[25] COMPTE RENDU DE L'AUDITION DE M. CÉDRIC O, SECRÉTAIRE D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES, *Mercredi 16 mars 2022*

[26] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

of intrusion into individuals' private lives and does not have a place in a democratic society as by their nature it entails mass surveillance"[27].

There is also strong opposition by European civil societies to the deployment of such techniques. The 'reclaim your face' campaign was launched by a consortium of NGOs including 'La Quadrature du Net', 'Homo Digitalis', 'The Hermès Center for Transparency and Digital Human Rights', calling for a ban on biometric surveillance techniques in public spaces[28].

Beyond the issue of human rights, the decision as to whether facial recognition should be deployed to monitor major events such as the Olympic games should be based on an assessment of the efficiency of such technology. In France, the Nice Carnival experiment, which was limited in terms of the time it took and the area that it covered, was the only French FRT trial in public places carried out for identification purposes. However, in the United Kingdom, the South Wales Police (SWP) and the London Metropolitan Police (LMP) have both experimented with the use of facial recognition to monitor public places in an operational context[29].

These two experiments in the UK gave rise to two evaluation reports drafted by two independent research centres. The exact results of these studies lay beyond the scope of our paper however it is worth mentioning that in operational environments they showed pretty poor results[30].

Against this background, having considered not only the legal issues around facial recognition technology deployed in public places but also the ethical issues concerning a technology which is not accepted by the whole population, and which can be misused, the French Government decided to reject the use of facial recognition during the 2024 Olympic Games.

As a matter of fact, the first draft of the law on the 2024 Olympic and Paralympic Games as presented to the Council of Ministers contains no mention of facial recognition – even for verification purposes – whatsoever. Indeed, article 7 of the bill which deals with the implementation of AI-enabled smart cameras only mentions that *"(t)hese processing operations do not use any biometric identification system, do not process any biometric data*

[27] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, May 12th, 2022, available at: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

[28] Reclaim Your Face campaign website, available at: https://reclaimyourface.eu/

[29] Including to monitor sports events, in the context of the South Wales Police experiments.

[30] See DAVIES (B.), INNES (M.), DAWSON (A.), "An Evaluation of South Wales Police's Use of Automated Facial Recognition", Universities' Police Science Institute Crime and Security Research Institute Cardiff University, September 2018, p.25, FUSSEY (P.), MURRAY (D.), "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", The Human Rights, Big Data and Technology Project, Human Rights Centre, University of Essex, July 2019, p. 70.

and do not use any facial recognition techniques. They may not be reconciled, interconnected or automatically linked with other personal data processing operations"[31].

Even though the French Government eventually abandoned its project to deploy facial recognition, it decided to permit the implementation of other AI-driven video devices to ensure the safety of sporting events during the Paris 2024 Olympic Games.

II. Smart cameras: a less invasive technology?

As previously mentioned, instead of deploying facial recognition technologies, the French Government intends to opt for another technology which is said to be less invasive. The main difference between smart cameras and facial recognition is that, while facial recognition's objective is to identify or authenticate an individual, smart cameras can have several objectives ranging from analysing to categorising objects or individuals.[32]

Following a two-month public consultation, the CNIL published an opinion on July 19th, 2022 on the deployment of smart cameras in public spaces. As briefly mentioned, CNIL defines this technology as video devices equipped with algorithmic processing to allow automatic analysis of images. The document focuses strictly on systems that are deployed in public spaces to "*analyse images in real-time and continuously*" to extract various types of information, leaving out of its scope technology that processes biometric data such as facial recognition technology.[33]

As explained in a senatorial information report, there are different ways in which AI-enabled systems can process images or a succession of images: first, some smart devices might be employed to "*detect the presence of an object or person in an image without determining its nature*".[34] Second, there are the systems used to recognise certain categories of images, such as types of objects or pedestrians (e.g. during the Roland-Garros tennis tournament in 2020, a trial was conducted to count the number of individuals in a queue and detect abnormal crowd movements).[35] The third type of AI-enabled system is used to identify an individual or an object based on non-biometric characteristics such as clothing (e.g. according to the report, the French railway company SNCF experimented with such a system for its "PREVIENS" project.).[36]

---

[31] PROJET DE LOI relatif *aux* jeux Olympiques *et* Paralympiques *de 2024,* December 22nd, 2023, available at: https://www.senat.fr/leg/pjl22-220.pdf

[32] CNIL, "Caméras dites « augmentées » dans les espaces publics : la position de la CNIL", *CNIL's Official website*, July 19, 2022, available at: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil

[33] CNIL*, "CAMÉRAS DITES "INTELLIGENTES" OU "AUGMENTÉES" DANS LES ESPACES PUBLICS. Position sur les conditions de déploiement", July 2022, available at: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf (Translated by DeepL.)*

[34] DAUBRESSE (M-P.), DE BELENET (A.), DURAIN (J.), Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, Sénat, 10 mai 2022,, available at : http://www.senat.fr/rap/r21-627/r21-6271.pdf

[35] *Ibidem*

[36] *Ibidem*

Finally, the fourth type of system (which will not be discussed here) aims to identify an individual by processing biometric data (e.g. facial recognition systems).

The main difference between smart cameras and facial recognition technology is that smart cameras do not process biometric data or are intended to identify individuals. However, even though smart cameras do not process biometric data this does not mean that they do not pose risks to an individual's liberties and human rights, since they could process other types of personal data. This also means that they should be considered more intrusive than "traditional" video surveillance systems since, as explained by the CNIL, smart cameras are by nature very different from traditional video-surveillance systems as "*people are no longer simply filmed, but analysed in an automated way, in real-time, to collect certain information about them*".[37] For example, systems that are deployed near health facilities or religious establishments could film and process the sensitive data of those individuals who attend these establishments. Furthermore, the French DPA considered that because of the "invisible" nature of this technology, and the fact that it can be deployed in existing video-surveillance systems, "generalised surveillance" can ensue due to massive processing of personal data.

Moreover, AI-enabled software can be easily deployed with existing video surveillance systems. Because of its nature, it can be "*integrated into places of very different natures (public roads, public transport, commercial, cultural and sports centers, etc.), with a geographical coverage, density requirements (a few cameras or a very meshed network) and very varied infrastructures (mobile, fixed, on-board, drone, portable, etc.) to pursue various objectives*".[38] These particular conditions could lead to multiple deployments in public spaces where it would "*undoubtedly present risks for the fundamental rights and freedoms of individuals and the preservation of their anonymity in the public space*".[39]

The risks smart camera systems pose depend on the objective and the way they are intended to be used. For example, a system that influences or makes a decision that individually affects a person does not pose the same risk as a system that targets an undetermined group of people or is deployed for statistical purposes.

In France there is no specific law regulating the use of smart cameras, however, this does not mean that the systems are not subject to regulation nor that they are *de facto* allowed or illegal. The French Internal Security Code regulates the use of "classic" video-surveillance systems that "capture images" but it does not cover "smart" video devices. The French DPA has explained that the internal security code intends to regulate only the devices that fall within its

[37] CNIL, "Caméras dit "augmentées" dans les espaces publics: la position de la CNIL, July 19th, 2022, available at: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil

[38] CNIL, *"CAMÉRAS DITES "INTELLIGENTES" OU "AUGMENTÉES" DANS LES ESPACES PUBLICS. Position sur les conditions de déploiement", July 2022, available at: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf (*

[39] CNIL : "Caméras dit "augmentées" dans les espaces publics: la position de la CNIL, July 19th, 2022, available at: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil

scope (i.e. traditional video surveillance systems) and does not prohibit the deployment of other devices.

Since smart video devices can be used in very different ways and are not subject to a specific regulation, CNIL has concluded that "*the analysis of the legality of the algorithmic processing on which the 'smart' video is based must therefore be carried out on a case-by-case basis*"[40]. For this case-by-case analysis, several factors should be taken into consideration, such as the place where it will be deployed, the purposes of the deployment, the information relating to individuals that the software will process, and so on.

Generally, if smart camera systems process personal data, their use must respect data protection principles and regulations: the French law on data processing and liberties (*loi informatique et libertés*), and the General Data Protection Regulation or the Law Enforcement Directive if the processing is carried out by law enforcement authorities. Additionally, the CNIL notes that a data protection impact assessment must be carried out "*because of the innovative nature of the technology*".[41] Furthermore, in certain specific cases data protection law provides for the need to adopt internal provisions, for instance when technology is used by law enforcement authorities to prevent crime. In such scenarios, smart video deployments "*require a legislative or regulatory text authorising or supervising them to be legally implemented*".[42]

As mentioned above, the French Government wants to deploy smart camera technology as a means of supporting security arrangements at the 2024 Olympic Games in Paris. A bill has been submitted to parliament to regulate the deployment of this technology during the Olympic Games. In an information report presented to the senate, the rapporteurs listed a series of ways in which the government could use these systems to assist security forces:

> *"-detect dangerous, prohibited or atypical materials that require the removal of doubt about their nature and dangerousness;*
>
> *- detect changes in the pace or direction of a crowd, a group or an individual within a crowd, or a vehicle or type of vehicle within traffic;*
>
> *- measuring the flow and density of people and vehicles to ensure compliance with public safety, civil or health regulations;*
>
> *-detecting certain characteristics of people, such as the wearing of face masking devices by an individual or group of individuals in a crowd, to enable the tracking of people considered to be potential threats.*"[43]

---

[40] CNIL,*"CAMÉRAS DITES "INTELLIGENTES" OU "AUGMENTÉES" DANS LES ESPACES PUBLICS. Position sur les conditions de déploiement",op. cit.*
[41] *Ibidem*.
[42] *Ibidem.*
[43] Rapport d'Information n° 776 (2021-2022) de MM. François-Noël BUFFET et Laurent LAFON, *fait un nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et*

In addition, in an information report following the security incidents at the Stade de France, the rapporteurs made a series of recommendations among which they suggest specifically providing a legal basis for experimenting with these systems. In particular, one of the recommendations suggests that the Minister of the Interior and the Parliament "*establish, on an experimental basis, the legislative basis that would allow operators of video protection systems in publicly accessible areas to implement image processing using artificial intelligence to count and detect crowd movements*"[44].

For the Olympic Games, smart camera technology would be deployed to ensure safety, falling within the competence of the State's "police-administrative" authorities. The use of smart cameras for security purposes can have an impact on individuals and their ability to exercise their civil liberties. As mentioned previously, "smart" devices should be considered more invasive than traditional video surveillance systems, especially when deployed for law enforcement purposes, hence the need for a law that specifically regulates their deployment. The French DPA explains that requiring a specific law before deploying smart devices for law enforcement purposes is based on an interpretation of Article 34 of the Constitution, which "*lays down the rules concerning civil rights and the fundamental guarantees granted to citizens for the exercise of public freedoms (...)*"[45]. With regard to this issue, the CNIL gave this explanation:

> "*Algorithmic processing for the detection of "suspicious" or unlawful behaviour entails a change of degree and nature in the remote surveillance of the public space that the legislator wished to regulate several years ago within the [Internal Security Code] for "traditional" video surveillance cameras. The new devices generate increased risks for individuals beyond the sole issue of protection."*[46]

In particular, the DPA considers that "*[o]nly a specific law, adapted to the technical characteristics and issues at stake, could possibly, after a democratic debate, decide on their legitimacy and, by setting minimum guarantees, provide for a balanced conciliation between*

---

d'administration générale sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, presented on May 10, 2022, available at : http://www.senat.fr/rap/r21-627/r21-6271.pdf

[44] Recommendation n° 11, Rapport d'Information n° 627 (2021-2022) de MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, *fait un nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) et de la commission de la culture, de l'éducation et de la communication (2) sur les incidents survenus au Stade de France le 28 mai 2022*, presented on July 13, 2022, available at : https://www.senat.fr/rap/r21-776/r21-7761.pdf

[45] Article 34, Constitution du 4 octobre 1958 en vigueur, available at: https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur

CNIL, "Consultation publique sur le projet de position de la CNIL relatif aux conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publiques. Synthèse des contributions de la consultation publique et réponses de la CNIL", July 2022, available at: https://www.cnil.fr/sites/default/files/atoms/files/consultation-publique-cameras-intelligentes-augmentees_synthese_des_contributions.pdf

[46] CNIL, *"CAMÉRAS DITES "INTELLIGENTES" OU "AUGMENTÉES" DANS LES ESPACES PUBLICS. Position sur les conditions de déploiement",op. cit.*

the objective of safeguarding public order and the imperative of protecting fundamental rights and freedoms."[47]

The CNIL's position seems to be shared by the Conseil d'Etat, which in an unpublished opinion also considered that an explicit legislative basis is needed for processing images from public spaces using artificial intelligence.[48]

Even though the bill which was submitted to the Senate only provides for experimentation that is supposed to end in June 2025, privacy campaigners fear that this technology will become permanent, in spite of their consideration that such real-time video analysis systems enable surveillance of public spaces[49].

Furthermore, the CNIL published an opinion on June 17th, 2020 concerning Datakalab,[50] a start-up that provided mask detection software during the Covid-19 pandemic. The CNIL also concluded on this occasion that *"when they constitute automated processing of personal data and are therefore covered by the GDPR, such systems most often lead either to the processing of sensitive data without the consent of the interested parties (in particular people's temperature being taken), or to the disregard of the right to object. In both cases, these devices must be subject to a specific regulatory framework, which will require upstream consideration of the proportionality of the use of such devices and the necessary guarantees".*[51] This opinion led to the adoption of Decree n° 2021-269 which regulates the use of mask detection systems[52].

As previously mentioned, the French Government did adopt a clear legal framework to authorise the deployment of smart video devices to support security arrangements at the Paris Olympic games, however the exact purpose for which such systems can be deployed remains unclear. Article 7 of the bill, which has been submitted to the Senate reads as follows:

"On an experimental basis and until 30 June 2025, for the sole purpose of ensuring the security of sporting, recreational or cultural events which, because of their scale or circumstances, are particularly exposed to the risk of acts of terrorism or serious attacks on the safety of individuals, images collected by means of video protection systems authorised on the basis of Article L. 252-1 of the internal security code and cameras installed on aircraft authorised on the basis of Chapter II of Title IV of Book II of the same code in places hosting these events

[47] *Idem*
[48] DAUBRESSE (M-P.), DE BELENET (A.), DURAIN (J.), Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, Sénat, 10 mai 2022, available at: http://www.senat.fr/rap/r21-627/r21-6271.pdf
[49] See KAYALI (L.), "France plots surveillance power grab for Paris 2024 Olympics", Politico, January 18th, 2023.
[50] Datakalab is a French start-up that during the Covid-19 pandemic provided RATP and the Cannes City Council a software capable of detecting if individuals were wearing a mask or not.
[51] CNIL, "La CNIL appelle à la vigilance sur l'utilisation des caméras dites 'intelligentes' et des caméras thermiques", June 17th, 2020, available at: https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras
[52] Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, JORF n°0060, March 11, 2021, available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043235679,

and in their surroundings, as well as in public transport vehicles and rights-of-way and on the roads serving them, may be subject to algorithmic processing for the sole purpose of detecting, in real time, predetermined events likely to present or reveal these risks and reporting them with a view to implementing the necessary measures by the police, predetermined events likely to present or reveal these risks and to report them with a view to the implementation of the necessary measures by the national police and gendarmerie services, the fire and rescue services, the municipal police services and the internal security services of the SNCF and the Régie Autonome des Transports Parisiens in the context of their respective missions"[53].

The text is deliberately vague since the bill expressly mentions that the conditions for the implementation of such systems and related data processing will be provided for in a further decree.

The CNIL's chair provided additional information about how exactly these smart video devices are intended to be used. In that respect, she claimed that *"(w)hat is planned in this bill is that, for the first time in France, in order to assist the decision-making of the public forces, there will be automatic real-time analysis of still images, for example, from video protection cameras or from drones, using algorithms and artificial intelligence to detect, for example, suspicious behaviour, incidents, abandoned parcels or crowd movements"*[54]. Once again, the exact purposes of these deployments remain vague but there is no doubt that parliamentary debates will clarify how these systems are going to operate.

As a conclusion, it is worth mentioning that, for the time being, there is no clear evidence about whether such smart video systems are efficient. There is very little information available about past experiments and their outcomes. For example, several local authorities in France are supposedly using artificial intelligence combined with video surveillance images to spot abandoned bags, monitor public transportation, modify traffic lights, etc. The municipality of Toulouse has experimented, according to an article by La Dépeche, with software that detects suspicious situations. However, following this trial the Deputy Mayor stated that the experimentation with smart cameras was not "totally satisfactory".[55]

[53] PROJET DE LOI relatif *aux* jeux Olympiques *et* Paralympiques *de 2024,* December 22nd, 2023, available at: https://www.senat.fr/leg/pjl22-220.pdf

[54] See "JO 2024 : la Cnil appelle les parlementaires à ne pas introduire de la reconnaissance faciale dans la loi", Francetvinfo, January 24th, 2023, available at: https://www.francetvinfo.fr/internet/video-jo-2024-la-cnil-appelle-les-parlementaires-a-ne-pas-introduire-de-la-reconnaissance-faciale-dans-la-loi_5620073.html

[55] EMERY (P.), "Toulouse : le pouvoir des caméras de vidéosurveillance", *La Dépêche*, January 3, 2019, available at: https://www.ladepeche.fr/article/2019/01/03/2934369-toulouse-le-pouvoir-des-cameras.html

These statements are attributable only to the author, and their publication here does not necessarily reflect the view of the other members of the AI-Regulation Chair or any partner organizations.

This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003)