

Facial Recognition Through the Lens of National Legislations - France*

Caroline Lequesne

(Associate Professor (HDR) in Public Law, Université Côte d'Azur, GREDEG CNRS UMR 7321)

ABSTRACT Although facial recognition technologies are extensively relied upon in judicial proceedings, their preventive deployment, particularly for crowd surveillance and management, remains highly exceptional in France. A limited number of pilot projects have been carried out, but these remain peripheral. In the absence of a dedicated legislative framework, the current legal regime is largely shaped by the safeguards articulated by the Conseil constitutionnel in its jurisprudence on surveillance technologies, alongside the applicable data protection rules. The adoption of the EU AI Act responds to long-standing legislative ambitions in France; however, efforts to establish a permanent national framework have stalled, primarily due to an unfavourable political climate.

KEYWORDS: Facial recognition technology (FRT) - Surveillance - Preventive policing - Data protection law - *Conseil constitutionnel* - Public space regulation - AI Act (EU) - Fundamental rights - National security

TABLE OF CONTENTS: 1. Introduction. – 2. Deployment of Facial Recognition Technologies in France. – 2.1. Real-Time Experiments. – 2.2. Retrospective Recognition: The Criminal Records Database (TAJ). – 2.3. Deployment Below the Radar: The Briefcam Case. – 3. The French Legal Framework for Facial Recognition in Public Spaces. – 3.1. Constitutional Safeguards. – 3.2. Data Protection Laws & biometric data. – 4. French perspectives for the Implementation of the AI Act. – 4.1. From the Olympic Experimentation Law to the Special Bill. – 4.2. The CNIL as the Competent Authority for Future Deployments.

1. Introduction

Spring 2025. In France, supermarket checkout lines have become the latest testing ground for biometric identification technologies. The new national AI frontrunner - Veesion - has turned its attention to combating shoplifting, promising retailers significant financial gains. Yet the legal trajectory is far from straightforward: stealthy deployment in a grey regulatory area, formal warnings from the French data protection authority (*Commission Informatique et Libertés, CNIL*), legal challenges before the *Conseil d'État*, and intensive lobbying to frame the technology as lawful. This pattern is neither new nor isolated - it typifies the legal dynamics surrounding facial recognition in France over the past six years. Across publicly accessible spaces, the facial recognition industry has sought to expand its footprint, subtly reshaping the social contract. Still, both cultural and legal resistance remain strong, and in the absence of a dedicated legislative framework, most pilot programs have not led to long-term implementation. For now, facial recognition remains largely restricted to the judicial context.

This article offers a practical and legal overview of the deployment of biometric identification technologies in public spaces in France. The first part examines the main areas

of deployment - whether experimental or judicial, in real time or retrospectively, and often operating below the radar (2); the second outlines the existing constitutional and legislative safeguards - particularly in the realm of data protection - that currently define the boundaries of any future regulatory framework (3); the third turns to the future, assessing how ongoing projects and the adoption of the EU Artificial Intelligence Act are shaping emerging regulatory pathways (4).

2. Deployment of Facial Recognition Technologies in France

2.1. Real-Time Experiments

Real-time facial recognition experiments in public spaces in France remain limited, due to existing legislative constraints. However, three domains of application have emerged as recurrent testing grounds and sources of public and political debate: cultural and sporting events, educational institutions, and stadiums.¹

The most widely publicized experiment took place in the city of Nice during its 134th

¹ We set aside airports, where facial recognition is deployed primarily for authentication purposes under a distinct legal framework and procedure. This specifically refers to the PARAFE system. Décret No. 2023-544 du 30 juin, 2023 portant modification des dispositions relatives au traitement automatisé de données à caractère personnel dénommé PARAFE.

* Article submitted to double-blind peer review.

annual carnival. Over three days (16, 19, and 20 February 2019), the city deployed facial recognition technologies in collaboration with the Israeli company AnyVision. The software was tested using the city's pre-existing CCTV infrastructure.² Two distinct trials were conducted. The first involved an authentication system at event entrances, based on participant consent. The second, referred to as "on-the-fly" identification, aimed to detect persons of interest within the crowd. The trial did not involve access to criminal databases; instead, it used scripted scenarios wherein the "individuals of interest" were municipal officers who volunteered and submitted their photos in advance. On-the-ground agents collected and relayed data to the city's Urban Supervision Centre. While the trial did not require prior authorization from the CNIL under the legal framework in place at the time, it nonetheless raised significant concerns about its legality. The use of "scientific research" as a declared purpose brought the experiment under the scope of the GDPR, thereby allowing reliance on consent as a legal basis. However, the CNIL questioned the conditions under which consent was obtained and requested additional information regarding potential algorithmic biases. The municipality submitted a detailed report. However, it was unable to provide key technical documentation, which fell under the purview of the private company.³ Following these exchanges, the CNIL concluded that the deployment of such technology in public spaces could not, in any case, continue in the absence of an appropriate legal basis.⁴ This marked the last officially conducted experiment involving real-time facial recognition in public space in France to date.

Often associated with cultural events, sporting venues - particularly stadiums - represent the second main context in which real-time facial recognition has been tested in

publicly accessible spaces in France. According to press reports, an experimental deployment was carried out by FC Metz in 2020.⁵ The initiative aimed, at minimum, to automatically identify individuals subject to stadium bans. It also included features for detecting abandoned objects and supporting counter-terrorism efforts. The CNIL determined that, under the legal framework in force at the time, the project was not compliant with either data protection law or the legal regime governing sports.⁶ This position effectively put an end to the trial and any related initiatives, although it did not entirely dampen interest in deploying such technologies. Figures such as the owner of Olympique Lyonnais continue to advocate for these systems, not only to improve stadium security but also - more explicitly - to generate additional revenue streams for clubs.⁷ The globalisation of sport plays a key role in promoting this commercial model, already in place in countries such as Brazil. Yet this approach has so far faced resistance in France.

It is also worth clarifying that, despite early announcements and popular belief, facial recognition was not trialled during the Olympic Games or the cultural and sporting events that preceded them. Nevertheless, the pilot project discussed below may offer insight into developments likely to emerge in the future.

The third high-profile facial recognition pilot concerned two high schools in the Provence-Alpes-Côte d'Azur region. Although never implemented, the initiative was ultimately blocked by a ruling from the Marseille Administrative Court. The project was part of the regional authority's "school safety plan", which involved the deployment

² *Expérimentation reconnaissance faciale*, Rapport de la ville de Nice, 2019, accessed online 2 May 2025, www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html.

³ M. Utersinger, *Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise*, in *Le Monde*, 28 August 2019, accessed online 2 May 2025, www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html.

⁴ CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux*, November 2019, 1-11, accessed online 2 May 2025, www.cnil.fr/sites/default/files/atom_s/files/reconnaissance_faciale.pdf.

⁵ *La reconnaissance faciale au FC Metz, une expérimentation qui suscite la controverse*, in *France 24*, 2 February 2020, accessed online 2 May 2025, www.france24.com/fr/20200202-la-reconnaissance-faciale-au-fc-metz-une-exp%C3%A9rimentation-qui-suscite-la-controverse.

⁶ CNIL, *Reconnaissance faciale et interdiction commerciale de stade : la CNIL adresse un avertissement à un club sportif*, 18 February 2021, accessed online 2 May 2025 www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club.

⁷ *La reconnaissance faciale comme solution face à la violence dans les stades ?* John Textor aimerait l'expérimenter au Groupama Stadium, Lyon Capitale, 14 January 2025, accessed online 2 May 2025: www.lyoncapitale.fr/actualite/la-reconnaissance-faciale-comme-solution-face-a-la-violence-dans-les-stades-john-textor-aimerait-l-experimenter-au-groupama-stadium.

of over 1,300 video surveillance cameras across public high schools. The proposal aimed to trial facial recognition technology at school entrances to achieve three objectives: streamlining access for authorised individuals, preventing identity fraud, and detecting or flagging unauthorised movements within school premises. According to the Data Protection Impact Assessment (DPIA) submitted to the CNIL, the system would have operated on two levels: “visual gateways” at school entrances to authenticate authorised individuals and an internal tracking mechanism within the school itself. Interestingly, the local council’s communications strategy adapted its messaging depending on the audience. Politically, the project was framed as enhancing security; legally, it was presented as a data management tool justified by its experimental nature and grounded in the General Data Protection Regulation (GDPR). The legal basis advanced for the data processing was student consent. The Marseille Administrative Court rejected this foundation, ruling that the hierarchical relationship between students and the educational institution undermined the possibility of obtaining freely given and informed consent.⁸ This conclusion aligned with the CNIL’s earlier opinion, which had found the project incompatible with the core principles of proportionality and data minimisation enshrined in the GDPR.⁹ Despite the legal and regulatory setbacks, public authorities have continued to advocate for the use of such systems in schools. The tragic school shooting in Nantes served as a renewed catalyst, with facial recognition technology and weapon-detection gates increasingly presented as viable solutions to pressing societal concerns.¹⁰

⁸ TA Marseille, 27 February 2020, no. 1901249.

⁹ CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position*, 29 octobre 2019, accessed online 2 May 2025, www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

¹⁰ E. Fernandez, *Attaque à Nantes: fouilles, portiques, reconnaissance faciale... Ces pistes évoquées pour renforcer la sécurité des écoles*, in *BFM*, 25 April 2025, accessed online 2 May 2025, www.bfmtv.com/police-justice/attaque-a-nantes-fouilles-portiques-reconnaissance-faciale-ces-pistes-evoquees-pour-renforcer-la-securite-des-ecoles_AV-202504250355.html.

2.2. Retrospective Recognition: The Criminal Records Database (TAJ)

The use of facial recognition technologies a posteriori¹¹ is permitted under specific procedural frameworks. The Criminal Records Processing System (Traitement d’antécédents judiciaires - TAJ), established under Articles 230-6 to 230-11 of the French Code of Criminal Procedure, is employed in the context of judicial investigations (for identifying suspects) and administrative inquiries (such as background checks for certain public or sensitive positions). Data are collected by the national police services, national gendarmerie units, or customs officers authorized to perform judicial police functions. Among these data are photographs with technical characteristics that enable the use of facial recognition tools. Such data are recorded for individuals implicated in criminal proceedings,¹² as well as those subject to judicial inquiries into the causes of death, serious injury, or disappearance.¹³

Created in 2012 through the merger of several pre-existing databases, TAJ constitutes one of France’s largest police data repositories. According to the CNIL, it contains information on nearly 87 million cases and covers approximately 18.9 million individuals, roughly 30% of the French population. A 2018 parliamentary report indicated that between 7 and 8 million facial images were stored in the database.¹⁴ Although the use of facial recognition technologies requires a demonstration of “absolute necessity,”¹⁵ its application appears

¹¹ The distinction between real-time and retrospective facial recognition can be difficult to draw. For a detailed discussion of the related issues, see C. Jasserand’s contribution in this issue.

¹² Persons against whom, during a preliminary investigation, an investigation conducted in flagrante delicto, or under a letter rogatory, there is serious or consistent evidence making it likely that they participated- either as perpetrators or accomplices - in the commission of a felony, a misdemeanour, or a fifth-class infraction.

¹³ Within the meaning of Articles 74 and 74-1 of the Code penal (French Code of Criminal Procedure).

¹⁴ *Rapport d’information déposé en application de l’article 145 du règlement, par la commission des lois constitutionnelles, de la législation et de l’administration générale de la République, en conclusion des travaux d’une mission d’information sur les fichiers mis à la disposition des forces de sécurité*, no. 1335, 17 October 2018, accessed online 2 May 2025, www.assemblee-nationale.fr/dyn/15/dossiers/fichiers_disposition_forces_securite_rap-info.

¹⁵ See below.

to be widespread. The system was reportedly used for up to 1,200 facial recognition searches per day.¹⁶ Far from being exceptional, this use has been described as “an internal communication tool for law enforcement agencies, used to exchange as much practical information as possible”.¹⁷

This extensive use has drawn significant criticism regarding the relevance and accuracy of the information involved. In addition to systemic concerns regarding the technologies themselves, the quality of the input data has also been repeatedly questioned. As early as 2014, France was condemned by the European Court of Human Rights for its mismanagement of a predecessor database.¹⁸ A decade later, the CNIL issued a formal warning to both the Ministry of the Interior and Overseas France and the Ministry of Justice for poor management of the TAJ.¹⁹ It recalled that data must be rectified following judicial reclassification and erased, in principle, in the case of acquittals or dismissals.²⁰ However, these updates are often lacking, due to the absence of automatic communication from many public prosecutors’ offices to the TAJ database manager. As a result, records are not deleted or fail to include a note indicating a dismissal or acquittal. The CNIL denounced these issues as having “serious and concrete consequences for individuals”.²¹ It has instructed the relevant ministries to adopt corrective measures to improve data accuracy and ensure the effectiveness of individuals’ rights. The ministries have until 31 October 2026 to bring the system into compliance.

In the meantime, the use of facial recognition a posteriori within judicial procedures remains an integral part of routine law enforcement practice.

2.3. Deployment Below the Radar: The Briefcam Case

Facial recognition technologies have also reportedly been deployed in public spaces outside of legal frameworks and without public knowledge. A journalistic investigation published in November 2023 brought this issue to light.²² According to the media outlet Disclose, since 2015, France’s Ministry of the Interior and several municipalities had acquired video analysis software from the Israeli company BriefCam. As of 2018, the software is said to have been enhanced with facial recognition capabilities. While the system did not generate biometric templates capable of forming a standalone database,²³ it did allow for so-called “similarity searches”.²⁴ This feature enabled the identification and tracking of individuals based on various physical and clothing-related characteristics.²⁵ According to the report, the system was “actively used,” “in complete secrecy”, and “without judicial oversight or authorisation”²⁶ to monitor public spaces.

These revelations prompted an internal investigation initiated by the Ministry of the Interior and carried out jointly by the *Inspection générale de la police nationale (IGPN)*, the *Inspection générale de la Gendarmerie nationale (IGGN)* and the *Inspection générale de l’Administration (IGA)*.²⁷ In parallel, the CNIL conducted

²² G. Livolsi, M. Destal and C. Le Foll, *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale*, in *Disclose*, 14 November 2023, accessed online 2 May 2025, <https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale>.

²³ Much like Google Image Search, for instance, which relies on perceptual hashing or principal component analysis techniques.

²⁴ By analyzing the pixels generated by images to distinguish between moving ‘objects’ captured within the camera’s field of view - such as vehicles, people, animals, and so on.

²⁵ Inspection Generale de la Police Nationale, Inspection Generale de l’administration & Inspection Generale de la Gendarmerie Nationale, *Usage de logiciels d’analyse vidéo par les services de la police et la gendarmerie nationales*, hereinafter “Rapport interne”, February 2024, 33.

²⁶ G. Livolsi, M. Destal and C. Le Foll, *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale*, cit.

²⁷ The Inspection générale de la police nationale (IGPN), the Inspection générale de la Gendarmerie nationale (IGGN), and the Inspection générale de l’Administration (IGA) are French internal oversight bodies tasked with conducting inspections, audits, and investigations to ensure legality, efficiency, and integrity within the national police, gendarmerie, and

¹⁶ *Rapport d’information déposé en application de l’article 145 du règlement*, cit.

¹⁷ *Ibidem*.

¹⁸ European Court of Human Rights. (18 April 2013). *M.K. v. France* (Application No. 19522/09).

¹⁹ CNIL, *Délibération de la formation restreinte n°SAN-2024-017 du 17 octobre 2024 concernant le ministère de l’intérieur et des Outre-Mer et le ministère de la justice*.

²⁰ Unless the public prosecutor, or the designated magistrate, requests that it be retained.

²¹ Notably because it may influence the outcome of administrative inquiries conducted prior to entering a profession or being admitted to sit a civil service examination.

inspections of four Ministry of the Interior departments and eight municipalities. Civil liberties organisations also filed emergency legal actions (référé) seeking to halt the use of the software in the municipalities concerned.

It emerges from these proceedings that the use of facial recognition technology was relatively limited. According to statements by the relevant national and local authorities, no law enforcement body appears to have used real-time facial recognition in public spaces. Only one isolated instance of retrospective use was reported in the context of a judicial investigation. However, because the software was not formally classified as a facial matching tool, its use was not recorded in the official procedure. As a result, the Administrative Court of Nice did not order the municipality to suspend its use.²⁸

Nevertheless, the *CNIL* instructed the Ministry of the Interior to “disable or restrict the functionality,” which it deemed unlawful insofar as it remained accessible. This finding aligns with the internal investigation report, which concluded that the software’s underuse stemmed less from a lack of interest on the part of law enforcement than from administrative and informational shortcomings. The uncoordinated acquisition of the software by various agencies, the absence of a harmonized operational doctrine, and weak coordination between the police and gendarmerie were cited as key factors.²⁹ The report further emphasized that the adoption of video analysis software by law enforcement agencies responds to a “pressing need” to manage video surveillance streams and, more broadly, to test new digital tools. A sovereign, in-house system - referred to as “Système V” - is expected to be rolled out by 2026 to replace BriefCam.³⁰

Beyond questions of legality, the BriefCam case illustrates the strong institutional interest in facial recognition technologies and a pre-existing familiarity with surveillance tools. The core issue, however, remains the absence of a robust and comprehensive legal framework.

broader public administration, respectively.

²⁸ Tribunal administratif de Nice, 23 November 2023, no. 2305692.

²⁹ Rapport interne.

³⁰ *Ibidem*, annex 3.

3. The French Legal Framework for Facial Recognition in Public Spaces

3.1. Constitutional Safeguards

In the absence of a dedicated legal framework, the Conseil constitutionnel has not had the opportunity to rule directly on the use of facial recognition technologies. However, a joint reading of its case law on “vidéoprotection” and “vidéosurveillance”,³¹ on the one hand, and on the use of algorithmic processing by public authorities, on the other, allows us to identify a set of safeguards that the Court would likely expect in the event that a specific law was adopted.

To begin with, Article 34 of the French Constitution entrusts Parliament with the responsibility to “determine the rules concerning the fundamental guarantees granted to citizens for the exercise of public liberties”.³² On multiple occasions, the Conseil constitutionnel has recognised the intrusive nature of both vidéoprotection³³ and biometric technologies.³⁴ Their use in public spaces - especially for public security purposes - poses a potential threat to fundamental rights and freedoms, “including individual liberty and freedom of movement, which may be hindered by violations of the right to privacy”. At the same time, such systems may pursue constitutionally protected aims, notably the prevention of public disorder and the identification of criminal offenders. Reconciling these imperatives therefore requires legislative intervention.

The Conseil constitutionnel made clear, both explicitly and implicitly, that the use of facial recognition technologies cannot be

³¹ In everyday language (and political discourse), the term “vidéoprotection” is often contested due to its positively charged connotation, in contrast to “vidéosurveillance”, which is perceived as highlighting the technology’s intrusive nature. This contribution does not aim to settle this debate but instead follows the terminology used by the legislator, who also assigns distinct legal regimes to each term.

³² In the wording consistently used by the *Conseil constitutionnel*, as confirmed in its decision on algorithmic video surveillance (see below).

³³ Décision no. 94-352 DC du 18 janvier 1995, Loi d’orientation et de programmation relative à la sécurité, cons. 3; Décision no. 2010-604 DC du 25 février 2010, Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d’une mission de service public, cons. 23; Décision no. 2021-817 DC du 20 mai 2021, Loi pour une sécurité globale préservant les libertés, § 81.

³⁴ See, for instance, Décision no. 2012-652 DC du 22 mars 2012, Loi relative à la protection de l’identité.

inferred from legislative silence. Article L. 242-4 of the French Internal Security Code stipulates that drones “may neither capture sound nor conduct any automated matching, interconnection, or linking with other personal data processing systems, nor incorporate automated facial recognition technologies”. The Court further clarified that, to comply with the right to privacy, these provisions must not be interpreted as permitting the competent authorities to analyse drone footage using external facial recognition systems not embedded in the devices themselves.³⁵ The Court reached the same conclusion with respect to algorithmic video surveillance piloted during the Olympic Games. This interpretive approach also applies to online data processing: the Conseil constitutionnel has rejected any reading of existing legal provisions - whether concerning platform regulation³⁶ or the fight against tax fraud³⁷ - that would implicitly authorise the use of facial recognition technologies.

The deployment of surveillance technologies entails a distinct and heightened risk to fundamental rights. The Conseil constitutionnel has underscored the “intensity” of the infringements stemming from their operational capabilities. Regarding drones, the Court noted that “these devices are capable of capturing, in any location and without their presence being detected, images of a very large number of individuals and tracking their movements over a wide area”.³⁸ Similarly, algorithmic video surveillance (AVS) “conducts a systematic and automated analysis of these images, which can significantly increase the volume and accuracy of the information extracted from them”.³⁹ In its ruling on AVS, the Conseil constitutionnel stated - in language not previously used - that “the deployment of such surveillance systems must be accompanied by specific safeguards designed to protect the

right to respect for private life.”⁴⁰

The Conseil constitutionnel identifies six main categories of safeguards. Developed through a body of case law, they serve as a blueprint for legislative compliance regarding the regulation of surveillance technologies.

The first safeguard concerns the conditions for deployment and the specific purpose of data processing. The Conseil constitutionnel requires the presence of a particular risk of serious harm to public order, which, by definition, implies exceptional circumstances.⁴¹ For example, the Court has ruled that deploying surveillance technologies to ensure the safety of sports, cultural, or recreational events - which, due to their scale or circumstances, are particularly exposed to risks of terrorism or serious threats to the safety of individuals - is legitimate and proportionate”.⁴² Conversely, the mere risk of damage to property,⁴³ the prevention of minor offences,⁴⁴ or the indiscriminate enforcement of a mayoral police⁴⁵ order cannot justify the deployment of such technologies.

The second safeguard relates to the requirement for prior authorisation. While the law may permit the use of such technologies, each individual deployment must be authorised by the competent authorities.⁴⁶ This authorisation must be specifically justified and tailored to the specific circumstances. In the context of drone surveillance, the Conseil constitutionnel has required the application of a subsidiarity principle: authorisation may be granted “only after the prefect has ensured that the service cannot use other means less intrusive with respect to this right, or that the use of such other means would pose serious threats to the physical integrity of the officers”.⁴⁷ Authorisation must also define spatial and temporal limitations by specifying the geographical area to be monitored and the maximum duration of surveillance.⁴⁸ The duration must be proportionate to the length of the event being secured and may only be renewed if the conditions for its issuance

³⁵ Décision no. 2021-834 DC, Loi relative à la responsabilité pénale et à la sécurité intérieure, §30 The same applies to onboard cameras. §54.

³⁶ Décision no. 2024-866 DC du 17 mai 2024, Loi visant à sécuriser et à réguler l'espace numérique, §107.

³⁷ Décision no. 2019-796 DC du 27 Décembre 2019, Loi de finances pour 2020, §§ 79 - 96.

³⁸ Décision no. 2021-817 DC, cited above, §30.

³⁹ Décision no. 2023-850 DC du 17 Mai 2023, Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, (hereinafter the “AVS Decision”), §42.

⁴⁰ *Ibidem*, §33.

⁴¹ AVS Decision §55.

⁴² *Ibidem*, §37.

⁴³ *Ibidem*.

⁴⁴ Décision no. 2021-817 DC, cited above, §139.

⁴⁵ *Ibidem*, §51.

⁴⁶ Regarding administrative policing, authority lies with the State representative in each département and, in Paris, with the Prefect of Police.

⁴⁷ Décision no. 2021-834 DC, cited above, §27.

⁴⁸ Décision no. 2021-817 DC, cited above, §130.

remain satisfied.⁴⁹ The issuing authority is furthermore required to terminate the authorisation immediately if the original conditions are no longer met.⁵⁰ Finally, the authorisation must also specify the types of systems authorised for deployment.⁵¹

The third safeguard concerns public notification. Access to information is a core element of algorithmic accountability, and the Conseil constitutionnel has affirmed its constitutional value in its decision on the automated allocation of university placements.⁵² In the context of surveillance, the Court requires that, “except where circumstances prohibit it or where such disclosure would conflict with the objectives pursued, the public must be informed in advance, by any appropriate means, of the use of algorithmic processing of the collected images”.⁵³ During the Olympic surveillance trial, the Conseil constitutionnel highlighted the relevance of a two-tiered approach to public information: both on-site notification at the time of deployment and a general information campaign “organised by the Ministry of the Interior”.⁵⁴

The fourth safeguard pertains to the technical characteristics of the systems. The Conseil constitutionnel requires that these features be precisely defined and must not include any ancillary functionalities that have not been explicitly authorised and safeguarded by law. For example, drones may not be used to capture images from inside private dwellings, and specific safeguards must be implemented where there is a risk of such intrusions.⁵⁵ Furthermore, drones may not capture audio, interconnect with other personal data processing systems, or include

automated facial recognition functionalities.⁵⁶

The fifth safeguard complements the fourth and concerns the implementation and operation of such systems. The Conseil constitutionnel requires safeguards for objective criteria, data types, and risk management protocols,⁵⁷ while also mandating human oversight. It established its guiding principle in this area as early as 2003, in a decision concerning the deployment of automated systems in judicial proceedings, stating that “no administrative or private decision involving an assessment of human behaviour may be based solely on automated processing of information used to define the profile or personality of the individual concerned”.⁵⁸ The exclusive reliance on algorithms is a fortiori excluded when sensitive data are processed.⁵⁹ Accordingly, in its decision on AVS, the Conseil constitutionnel emphasised that such processing alone must not ground any individual decision or any prosecutorial action and must be continuously overseen and governed by human agents.⁶⁰ It is therefore the responsibility of the legislator to ensure that the design, deployment, and evolution of algorithmic systems always remain under the control and supervision of human persons.

The sixth safeguard applies more specifically to experimental schemes and imposes additional accountability requirements. The Conseil constitutionnel indicated that, in deciding whether to make an experimental regime permanent after the expiry of the trial period, it would be incumbent on the legislator “to draw conclusions from the evaluation of the experimental scheme, and in particular, with regard to its impact on the right to privacy, to consider its effectiveness in preventing threats to public order”.⁶¹ Based on that evaluation, “the constitutionality of the scheme may then be subject to further review”.⁶²

Based on the Conseil constitutionnel’s evolving positions, adopting a dedicated law to authorise the use of facial recognition in publicly accessible spaces would likely entail

⁴⁹ Décision no. 2021-834 DC, cited above, §28.

⁵⁰ *Ibidem*.

⁵¹ Restrictions on how many camera-equipped drones may be used and on the maximum number of cameras permitted to operate at the same time.

⁵² The *Conseil Constitutionnel* recognised that the right of access to administrative documents holds constitutional value and ruled that documents relating to the characteristics and conditions of implementation of algorithmic processing constitute such documents. Moreover, the right of access was extended to third parties. Décision no. 2020-834 QPC du 3 avril 2020, *Union nationale des étudiants de France* (disclosure and accessibility of algorithms used by higher education institutions for reviewing applications for admission to undergraduate programmes).

⁵³ AVS Decision, §40.

⁵⁴ *Ibidem*.

⁵⁵ Décision no. 2021-834 DC, cited above, §29.

⁵⁶ *Ibidem*, §30.

⁵⁷ AVS Decision, §44.

⁵⁸ Décision no. 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, §§ 34 and 46.

⁵⁹ Décision no. 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*, §70.

⁶⁰ AVS Decision, §44.

⁶¹ Décision no. 2019-796 DC, cited above, §48.

⁶² *Ibidem*.

six core requirements. First, such use would need to respond to exceptional circumstances involving serious threats to public order. Second, deployments would have to be individually authorised by competent authorities, based on strict necessity and proportionality. Third, the public would need to be informed in advance, unless compelling reasons justify an exemption. Fourth, the technical features of the systems would have to be narrowly defined by law, excluding any ancillary or unauthorised functionalities. Fifth, operational safeguards would be required, including human oversight, objective processing criteria, and risk mitigation procedures. Finally, in the case of experimental deployments, a robust framework for evaluation and democratic accountability would be necessary, with legislative reconsideration contingent on effectiveness and respect for fundamental rights.

3.2. Data Protection Laws & biometric data

Facial recognition technology estimates the likelihood of a match between an individual's facial features and their civil identity. It relies on the use of biometric data. In accordance with European legislation⁶³ - and in line with previous French practice⁶⁴ - biometrics are defined as a type of data processing (1) that exclusively handles bodily data (2). This includes physical, biological, and even behavioral traits that enable the automated identification of individuals. Under French law, biometric data are classified as personal data and subject to specific legal frameworks. They may either fall under the category of sensitive personal data, which is subject to stricter regulation, or be governed by a dedicated *ad hoc* regime. The applicable legal regime depends on the "informational density"⁶⁵ of the data: the higher the density, the stronger the protection of individual rights, which, in turn, warrants the adoption of

specific legal provisions. This rationale underpins the special legislative and regulatory frameworks that apply to genetic⁶⁶ and fingerprint data.⁶⁷ Similarly, advances in facial recognition technologies in France prompted the introduction of a legislative proposal.⁶⁸

In the context of special legal regimes, a distinction must be drawn between biometric processing carried out by the State in the exercise of its sovereign powers and other types of processing. Pursuant to Article 32 of the French Data Protection Act (*Loi Informatique et Libertés, LIL*⁶⁹), the former requires authorization by a decree of the *Conseil d'Etat*, issued following a reasoned and published opinion the *CNIL*. The data controller shall carry out a data protection impact assessment.⁷⁰ The "Criminal Records Processing" database (TAJ), previously mentioned, was established under this regime.⁷¹

In the context of criminal investigations, biometric data processing may be authorized under the specific conditions set out in Article 88 of the LIL, as amended to implement the Law Enforcement Directive. Biometric identification techniques, including facial recognition, may be used where their purpose is to identify the perpetrators of criminal offences. Such use must be necessary to protect rights and principles of constitutional

⁶³ On this point, see contribution by C. Jasserand in the present issue.

⁶⁴ Under French law, biometrics have been addressed in a unified manner since 2004 through the concept of "biometric processing". Loi No. 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁶⁵ M. Sztulman, *La biométrie saisie par le droit public, étude sur l'identification et la localisation des personnes physiques*, Paris, LGDJ, 2019, 11.

⁶⁶ This legal framework was established by the major bioethics laws of 1994, which include Loi No. 94-548 du 1 juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et la Loi No. 94-654 (concerning the processing of personal data for health research purposes) and Loi No. 94-654 du 29 juillet 1994 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal. (concerning the donation and use of human body elements and products, medically assisted reproduction, and prenatal diagnosis).

⁶⁷ Décret no. 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.

⁶⁸ Which was ultimately abandoned following a change in the majority in the National Assembly. Proposition de loi No. 4127 d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle.

⁶⁹ Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, hereinafter LIL.

⁷⁰ Article 90 of the LIL.

⁷¹ Articles R. 40-23 à R. 40-34 of the Code de procédure pénale (French Criminal Law Code).

value, which corresponds to the requirement of “absolute necessity” under this law. Moreover, this necessity may, in urgent circumstances, justify the use of such techniques by investigators without prior authorization from a judicial authority. The French *Cour de Cassation* has ruled that the interference with the right to privacy resulting from the use of facial recognition is justified by the legitimate aim of prosecuting offenders and is proportionate to the intended purpose.⁷² This proportionality is considered to be safeguarded, first because only the personal data of individuals convicted of the most serious offences may be stored in the database used for facial recognition, and second because judicial oversight is available. A judge, when seized by a motion to annul evidence, can review whether access to the database was limited to duly authorised officials.

For other types of processing, the *CNIL* is responsible for developing “standard regulations” (*règlements types*), which prescribe “additional technical and organizational measures”.⁷³ Compliance with these regulations is mandatory for any entity wishing to implement a biometric system within the relevant scope. In this context, the *CNIL* has adopted a standard regulation concerning the use of biometrics in the workplace.⁷⁴ This regulation more broadly sets out the *CNIL*’s position on biometrics, requiring organizations to justify the necessity of biometric systems, to document the technical choices made, to comply with strict security specifications (both organizational and technical), and to conduct a data protection impact assessment. Under this framework, the lawfulness of biometric processing depends on its intended use. Consent may permit private uses, subject to specific conditions, particularly regarding data storage. However, there is currently no legal basis allowing for the real-time deployment of facial recognition technology for security purposes in public spaces.

The *CNIL* promotes a case-by-case approach, requiring that any processing meet

the criteria of necessity, specificity, and proportionality.⁷⁵ Accordingly, the *CNIL* approved certain uses in principle - such as the system for airport border controls (« *Passage Automatisé Rapide Aux Frontières Extérieures* », *PARAFE*)⁷⁶ and the *ALICEM* system for digital identity verification⁷⁷ - while imposing strict conditions on their practical implementation. Conversely, it rejected other applications, including the use of facial recognition technology for student access control in schools.⁷⁸

4. French perspectives for the Implementation of the AI Act

4.1. From the Olympic Experimentation Law to the Special Bill

As suggested by the analysis of the Conseil constitutionnel’s case law on algorithmic video surveillance,⁷⁹ the adoption of experimental measures during the 2024 Olympic Games was conceived as an initial step toward enacting legislation on biometric identification in publicly accessible spaces. Although the use of facial recognition was not permitted during the Games, several factors support this interpretation.

Firstly, one year earlier, as part of its examination of Olympic security, the French Senate initiated a cross-party inquiry into facial recognition technologies. Although the *CNIL*’s president expressed a degree of openness, significant legal uncertainties persisted. As reflected in the final report of the Senate commission,⁸⁰ legislators feared that these uncertainties, combined with public opposition, would ultimately prevent the

⁷⁵ *CNIL, Reconnaissance faciale, Pour un débat à la hauteur des enjeux*, cit.

⁷⁶ Articles R. 232-6 to R. 232-11 of the Code de la sécurité intérieure (French Internal Security Code).

⁷⁷ Décret no. 2019-452 du 13 mai 2019 autorisant la création d’un moyen d’identification électronique dénommé “ *Authentification en ligne certifiée sur mobile* “, Conseil d’État, Chambres réunies, Décision no. 432656 du 4 novembre 2020.

⁷⁸ *CNIL, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position*, cit.

⁷⁹ See above.

⁸⁰ M.-P. Daubresse, A. de Belenet and J. Durain, *Rapport d’information au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d’administration générale sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles* (Sénat, Session ordinaire 2021-2022, no. 627, 10 May 2022), www.senat.fr/rap/r21-627/r21-6271.pdf, accessed 2 May 2025.

⁷² Cass, Crim., 9 October 2024, no. 24-80.871.

⁷³ Article 8 of the LIL.

⁷⁴ Délibération no. 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d’accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.

passage of dedicated legislation. As a result, lawmakers opted against this path for the Olympics, favoring alternative AI technologies for crowd surveillance that not allowed biometric identification.

Secondly, and as a result, the technologies tested under this law were closely related to facial recognition systems. They relied on similar tools, including sensors, cameras, and automated processing software. Furthermore, although these systems were less granular than biometric identification, they operated on the same fundamental logic: capture, categorization, and alert generation. The law authorized systems to detect “predefined events likely to present or reveal risks and to alert law enforcement authorities for the implementation of necessary measures.”⁸¹ A subsequent decree specified the nature of such events: the presence of abandoned objects; the presence or use of weapons, as listed under Article R. 311-2 of the Code de la sécurité intérieure (French Internal Security Code); violations of designated traffic flows by individuals or vehicles; unauthorized crossing or presence of individuals or vehicles in restricted or sensitive areas; individuals lying on the ground after a fall; crowd movements; excessive crowd density; and the outbreak of fires.⁸²

In this regard, the Olympic experimental law served as a significant precedent, both sociologically and legally, paving the way for potential future legislation specifically addressing biometric identification. On the practical side, the law anticipated the implementation of the AI Act by designating competent authorities and establishing procedures for authorization. However, it can be regretted that decision-making power was heavily concentrated within the executive branch: the prefectures were designated as the primary oversight bodies, empowered to authorize deployments and solely responsible for terminating ongoing operations in the event of risks to public liberties. The CNIL’s

role was merely advisory and relatively secondary.

One particularly notable and commendable innovation was the introduction of external accountability mechanisms.⁸³ The legislature mandated the creation of an ad hoc evaluation committee composed of two groups: one comprising “user services” (police forces, transport, and security services involved) and another made up of “independent and qualified individuals” selected for their expertise in personal data protection, digital technologies, and civil liberties.⁸⁴ The committee began its work even before the experiments, starting in February 2024. Its tasks included collecting detailed feedback from users, carrying out site visits and interviews during each experiment on behalf of the independent members, and facilitating regular discussions both within the independent group and in plenary sessions.

The goal was to develop an evaluation protocol aimed at delivering an assessment on: “1) the technical performance of the algorithmic systems deployed; 2) the operational effects of using such systems to secure the relevant events; 3) the impact of the algorithmic systems on safety and the exercise of civil liberties, as well as public perceptions of such impacts.” The resulting evaluation report documented “the number of requests for authorization to use algorithmic systems” and “alerts generated by the systems”, assessed “the impact of these systems on the safety of the events concerned,” and analyzed “the observed benefits or encountered challenges”.⁸⁵ It further reviewed “the conditions under which the public was informed and the rights of data subjects were upheld,” and evaluated “the level of public and user satisfaction and trust”.⁸⁶ This process represented an ongoing effort to (re)integrate the deployment of policing technologies into democratic scrutiny.

In this light, the outcome illustrated that these democratic mechanisms are indeed at work: despite political expectations, the

⁸¹ Loi No. 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, article 10.

⁸² Décret no. 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l’article 10 de la loi No. 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, Article 3.

⁸³ For more details, C. Lequesne, *IA et ordre public*, in *Revue Française de Droit Administratif*, 1, 2025.

⁸⁴ Décret no. 2023-939 du 11 octobre 2023 relatif aux modalités de pilotage et d’évaluation de l’expérimentation de traitements algorithmiques d’images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs.

⁸⁵ *Ibidem*, Article 4.

⁸⁶ *Ibidem*.

evaluation produced mixed results, which ultimately argued against making the technology permanent. Given the absence of conclusive results, the French government is now seeking to renew experimental deployments rather than formally integrating the technology into permanent security frameworks. In the preparatory work for the legislation concerning the 2030 Olympic Games,⁸⁷ both the legislature⁸⁸ and the Conseil d'État⁸⁹ adopted a similar stance: the added value of these technologies still needs to be demonstrated before their long-term integration into security frameworks can be justified.

Thus, the French legislative process has made progress in shaping the regulatory frameworks required under the AI Act, yet it currently remains at an intermediate stage of democratic deliberation. To date, however, two legislative proposals aiming to establish such a framework⁹⁰ have not come to fruition. The Minister of the Interior and the Minister of Justice continue to advocate strongly for the preventive deployment of facial recognition technology in public spaces. Nevertheless, the government's ambitions are tempered by the absence of a parliamentary majority.

4.2. The CNIL as the Competent Authority for Future Deployments

The AI Act further requires Member States to designate national market surveillance authorities. At the time of writing, France's institutional choices in this area remain somewhat unsettled. Since 2021, the CNIL, together with its European counterparts, has positioned itself within the institutional debate

as the principal authority for AI oversight.⁹¹ To this end, it established an internal "Artificial Intelligence Service" in 2023 and published an AI action plan. In 2022, the Conseil d'État also recommended a "profound transformation of the CNIL into a national supervisory authority responsible for regulating AI systems, particularly those deployed in the public sector".⁹²

During the three years of discussions surrounding the drafting and adoption of the AI Regulation, other institutional actors have emerged, such as ARCOM, and are ultimately expected to help shape a coordinated national regulatory model for AI governance. Nevertheless, the CNIL has retained its leadership on specific issues relating to biometrics and facial recognition, as illustrated by its recent positions on the deployment of behavioural recognition systems at retail checkouts.

Moreover, Article 74.8 of the AI Act specifies that "for high-risk AI systems listed in point 1 of Annex III to this Regulation, in so far as the systems are used for law enforcement purposes, border management, and justice and democracy, and for high-risk AI systems listed in points 6, 7, and 8 of Annex III to this Regulation, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Regulation (EU) 2016/679 or Directive (EU) 2016/680". In other words, the CNIL appears poised to serve as the competent authority responsible for overseeing biometric identification systems deployed in public spaces.

France is therefore moving towards establishing both a legal framework and governance structure for biometric identification systems, although democratic resistance continues to impede their permanent deployment.

⁸⁷ Projet de loi relatif à l'organisation des Jeux Olympiques et Paralympiques de 2030 (Session ordinaire 2024-2025, no. 158, 24 June 2025).

⁸⁸ Sénat, *Étude d'impact, projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024* (no. 220, Session ordinaire 2022-2023), www.senat.fr/leg/etudes-impact/pjl22-220-ei/pjl22-220-ei.pdf, accessed 21 May 2025.

⁸⁹ Conseil d'État, *Avis sur un projet de loi relatif à l'organisation des Jeux Olympiques et Paralympiques de 2030 et pérennisant certains dispositifs institués lors des Jeux Olympiques et Paralympiques de 2024* (6 May 2025).

⁹⁰ Proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle, no. 4127, déposée le mardi 4 mai 2021; Proposition de loi, adoptée par le Sénat, relative à la reconnaissance biométrique dans l'espace public, no. 1342, déposée le lundi 12 juin 2023.

⁹¹ Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

⁹² Conseil d'État, *S'engager dans l'intelligence artificielle pour un meilleur service public* (24 August 2022), www.conseil-etat.fr/actualites/s-engager-dans-l-intelligence-artificielle-pour-un-meilleur-service-public, accessed 21 May 2025.

