FACIAL RECOGNITION BETWEEN PRIVATE AND PUBLIC: GDPR, AI ACT AND NEW NATIONAL RULES

Artificial Intelligence & Data Protection

AUTORI

Aurora Agostini
Partner

Alessandro Carlini
Associate

Facial recognition systems involve the processing of biometric personal data and, as a rule, the use of an artificial intelligence system: Regulation (EU) 2016/679 ("**GDPR**") and Regulation (EU) 2024/1689 ("**AI Act**"), together with the related implementing decrees and regulations, therefore apply concurrently.

The year 2026 has profoundly reshaped the regulatory framework: the national moratorium in places that are public or open to the public has been extended to 31 December 2027; Legislative Decree No. 160 of 9 September 2026 lays down the rules governing use by the police forces; the subsequent Legislative Decree No. 179 of 7 October 2026 completes it as regards supervisory and sanctioning powers; Regulation (EU) 2026/1744 ("**Digital Omnibus**") has postponed to 2 December 2027 the obligations for high-risk systems in Annex III, including biometric systems, without prejudice to the prohibitions already applicable.

Where do we stand, then? May companies and employers use facial biometric recognition systems? And within what limits may law-enforcement authorities rely on these technologies?

BIOMETRIC DATA AND FACIAL RECOGNITION

Before examining the regulatory framework, a premise is appropriate: not all video-surveillance systems entail a processing of biometric data, nor does every processing of biometric data, in itself, give rise to a facial recognition system.

Pursuant to **Article 4(14) GDPR**, **"biometric data"** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm that person's unique identification, such as facial images. Video footage or a photograph of a person is therefore not, in itself, biometric data, as it is "raw" data; it only becomes biometric data following specific technical processing aimed at uniquely identifying the individual (*cf.* Recital 51 GDPR). Put differently, biometric data are present when three elements coexist: (i) the particular **nature** of the personal data (data relating to the physical, physiological or behavioural

characteristics of a natural person); (ii) the **means and methods** of processing applied to such raw data ("specific technical processing"); and (iii) the **purpose** of the processing (the data must be used to uniquely identify a natural person).

Precisely because of their sensitivity and impact on fundamental rights, biometric data fall within the **special categories of personal data under Article 9 GDPR**, whose processing is in principle prohibited unless one of the conditions in paragraph 2 applies; paragraph 4 then allows Member States to lay down additional conditions, provided in Italy by **Article 2-*septies* of the Privacy Code**.

Examples of biometric data include, for instance, iris scans or dactyloscopic data and, for present purposes, facial data processed for the unique identification of a person: in this latter case we refer to facial recognition systems based on biometric data.

It should also be clarified that, in facial recognition systems, biometric processing occurs both (i) at the registration phase (enrolment), consisting of acquiring the data subject's biometric characteristics (e.g., facial features), and (ii) at the actual recognition phase, i.e., when the face is captured. It follows that even the mere extraction of the mathematical model of the face (template) constitutes processing of biometric data.

Three distinct functions of facial recognition systems must then be distinguished, each defined by Article 3 of the AI Act and subject to its own regime:

- **biometric verification (1:1)**, which checks that a person is in fact who they claim to be by comparing the face against a single template previously provided;
- **biometric identification (1:N)**, which compares the face against those contained in a database of multiple persons and which, if performed at a distance, may occur "in real time" or "*a posteriori*";
- **biometric categorisation**, which assigns a person to specific categories on the basis of that person's biometric data.

The risks associated with facial recognition are numerous and specific: unlike a password, biometric data cannot be replaced; the artificial-intelligence algorithms on which the system relies may generate false positives and false negatives, with potential bias across population groups and significant consequences for the data subject's rights and freedoms; finally, deployment in public spaces risks discouraging the exercise of freedom of assembly and expression.

THE PRIVATE CONTEXT: LEGAL BASES, EMPLOYMENT, AND PLACES OPEN TO THE PUBLIC

To process special categories of personal data, the controller (e.g., a company intending to install a facial recognition system) must identify a legal basis under Article 6 GDPR and, cumulatively, one of the conditions in Article 9(2) GDPR.

In business settings, the legitimising condition is generally the data subject's **explicit consent** (point (a)), given freely, specifically, in an informed and unambiguous manner (Articles 4(11) and 7 GDPR), which presupposes, among other things, that a genuine, disadvantage-free non-biometric alternative is offered to the data subject.

A key distinction, drawn by the EDPB in Guidelines 3/2019, is between the use of facial recognition systems in uncontrolled environments and in controlled environments. In the former, the biometric device is placed in a public or publicly accessible space and operates on anyone entering the camera's field of view; in the latter, the system operates only with the active participation of a consenting person.

In uncontrolled environments, the system captures in real time the face of anyone entering the camera's field of view, including people who have not consented to the use of the biometric device, and generates the corresponding biometric templates. Those templates are then compared with those created by data subjects who gave prior consent during a registration process, so that the controller can recognise whether or not the person uses the biometric device. Even in these cases, one of the derogations under Article 9(2) GDPR must be relied upon which, as noted, in private contexts generally coincides with consent.

For places that are public or open to the public, moreover, **Article 9(9) of Decree-Law No. 139 of 8 October 2021** (as converted by Law No. 205 of 3 December 2021) suspends the installation and use of video-surveillance systems with facial recognition based on biometric data by public authorities and private entities until a statutory framework is adopted. The deadline was most recently extended to **31 December 2027** by Article 2(6-quater) of Decree-Law No. 200 of 31 December 2025, introduced upon conversion by Law No. 26 of 27 February 2026. While in the public context that framework may be found, as seen *infra*, in the national implementing provisions and, in particular, in Legislative Decree 160/2026, it currently appears difficult to envisage, at this stage, a lawful use of facial recognition systems in uncontrolled private environments—such as shops, malls, cinemas and private events—regardless of the legal basis relied upon.

As for **employment relationships**, the framework is even stricter: Article 4 of Law No. 300/1970 (Workers' Statute) allows the installation and use of devices from which the possibility of remote monitoring of workers may arise only for

organisational and production needs, workplace safety, and protection of company assets, subject to a trade-union agreement or authorisation by the labour inspectorate. In the workplace, therefore, the installation and use of video-surveillance systems are already in themselves subject to the labour-law safeguards of Article 4 of Law No. 300/1970, in addition to data-protection rules (notice obligations, a DPIA on the system, etc.). The Italian Data Protection Authority (*Garante per la protezione dei dati personali*) has, moreover, already ruled on facial recognition systems used for attendance recording (see Decision No. 108/2024), prohibiting the processing of employees' biometric data for attendance and clarifying that even consent is generally not a valid basis, given the asymmetry between employer and worker.

In our view, in private contexts, only 1:1 verification uses in controlled environments (not open to the public) remain conceivable—such as access to restricted areas—and only where there is explicit consent, a genuine alternative, a formalised DPIA and, preferably, templates under the data subject's control, without prejudice to what is noted for employer–employee relationships.

AI ACT AND ITALIAN LAW: RULES FOR BUSINESSES

As noted, the AI Act complements the GDPR and addresses both private and public actors in regulating biometric systems that use artificial-intelligence technologies.

The **prohibitions on developing and putting into service certain artificial-intelligence systems under Article 5(1) AI Act** also apply to businesses: creating or expanding facial-recognition databases by indiscriminate scraping of images from the internet or CCTV footage; emotion inference in the workplace and in educational institutions, save for medical or safety reasons; biometric categorisation to infer race, political opinions, trade-union membership, religious or philosophical beliefs, sex life or sexual orientation.

Under the heading of artificial-intelligence systems classified as high risk in **Annex III, point 1, AI Act**, and therefore subject to particular precautions, we find: (a) remote biometric identification systems, (b) categorisation based on sensitive attributes and (c) emotion recognition, while expressly excluding 1:1 verification. It follows that an access-control system based on facial verification is not high risk, while remaining fully subject to Article 9 GDPR, to data-protection rules as a whole and to the applicable limits under Union or national law.

The *deployer* of a high-risk system is required, among other things, to use it in accordance with the instructions for use, ensure competent human oversight, keep logs and inform workers and their representatives before commissioning it in the workplace. By virtue of the Digital Omnibus many of these obligations will, however, apply only from **2 December 2027**.

THE PUBLIC CONTEXT: CRIME CONTROL AND LEGISLATIVE DECREE 160/2026

Article 5(1) AI Act prohibits, among other things, "real-time" remote biometric identification in publicly accessible spaces for law-enforcement purposes, unless it is strictly necessary for the targeted search for victims of abduction, trafficking or sexual exploitation and missing persons; to prevent a specific, substantial and imminent threat to the life or physical safety of persons or a real and present, or real and foreseeable, threat of a terrorist attack; or to locate or identify suspects of the offences listed in Annex II to the AI Act that are punishable by a maximum term of at least four years' imprisonment or a security measure depriving liberty.

Even in such cases, a FRIA, registration of the system in the EU database, prior authorisation by a judicial authority or an independent administrative authority, notification to the market-surveillance authority and to the Italian DPA, and an enabling national law are required. "*A posteriori*" identification in targeted investigations requires authorisation to be requested within 48 hours, save for the initial identification of a potential suspect based on directly verifiable objective facts connected to the offence; the **FRIA** under Article 27 AI Act applies to public-law bodies and private entities providing public services and may complement the DPIA already carried out on the biometric system.

At national implementing level, the legal basis is currently provided by **Legislative Decree No. 160 of 9 September 2026**, adopted under Law No. 132 of 23 September 2025, which structures the discipline of facial recognition systems, in summary, as follows:

- **real time for prevention and search for victims or missing persons**: authorisation by the chief public prosecutor of the court of appeal district, upon request by the provincial police commanders (State Police, Carabinieri, Guardia di Finanza), for up to 15 days, renewable, in a delimited area; validation within 24 hours in urgent cases; database created for the single use and then deleted, with no scraping; prior FRIA and DPIA, and logs kept for five years;
- **real time for investigation purposes** (by introducing new Article 359-*ter* of the Code of Criminal Procedure): authorisation by the judge for preliminary investigations upon request by the public prosecutor (in urgent cases, a reasoned decree by the public prosecutor subject to validation), for the offences in Annex II to the AI Act punishable by a maximum term of not less than four years' imprisonment and for the search for fugitives and victims;
- ***a posteriori***: for the targeted search for a suspect, authorisation by the judge for preliminary investigations, which the public prosecutor must request within 48 hours and on which the judge rules within the following 48 hours; without authorisation, only the initial identification *ex* Article 26(10) AI Act;

in places and events with public-order needs, images processed without biometric processing, stored for seven days and compared only after an offence; a general or untargeted use is prohibited;

- in case of breach: inadmissibility of the results and deletion of the data.

In our view, the decree can be read as the statutory framework capable of overcoming the moratorium on facial recognition systems, but only for police activities: for private actors, nothing appears to have changed.

CONCLUSIONS

In short, facial recognition is not governed by alternative regimes—one for private actors, one for public authorities—but by multiple layers of rules that apply cumulatively. For businesses the framework remains decidedly restrictive: in employment there is no genuine enabling statute; in places that are public or open to the public a moratorium applies until 31 December 2027; and some uses are absolutely prohibited.

For the police forces, Legislative Decree 160/2026 introduces authorisations, limits and safeguards whose practical application should be monitored closely.

The deferral to 2027 of obligations for high-risk systems should not induce postponement of compliance: DPIAs, prohibitions, transparency obligations and national rules are already fully operational.

LEXIA's Data & Technology Innovation team remains available for any further analysis and to support companies and public entities in assessing facial recognition projects and related compliance roadmaps.

AUTHORS



Aurora Agostini

Partner



Giulietta Minucci

Partner



Marco Grechi

Senior Associate



Giovanni Lombardi

Associate



Alessandro Carlini

Associate



Francesca Costarelli

Associate

This document is provided for general information only and is not intended to constitute legal advice on the matters addressed. Recipients of this document may not rely on its contents. Neither LEXIA nor any of its professionals shall be liable in any way for the contents of this document, whether on the basis of an engagement or otherwise.