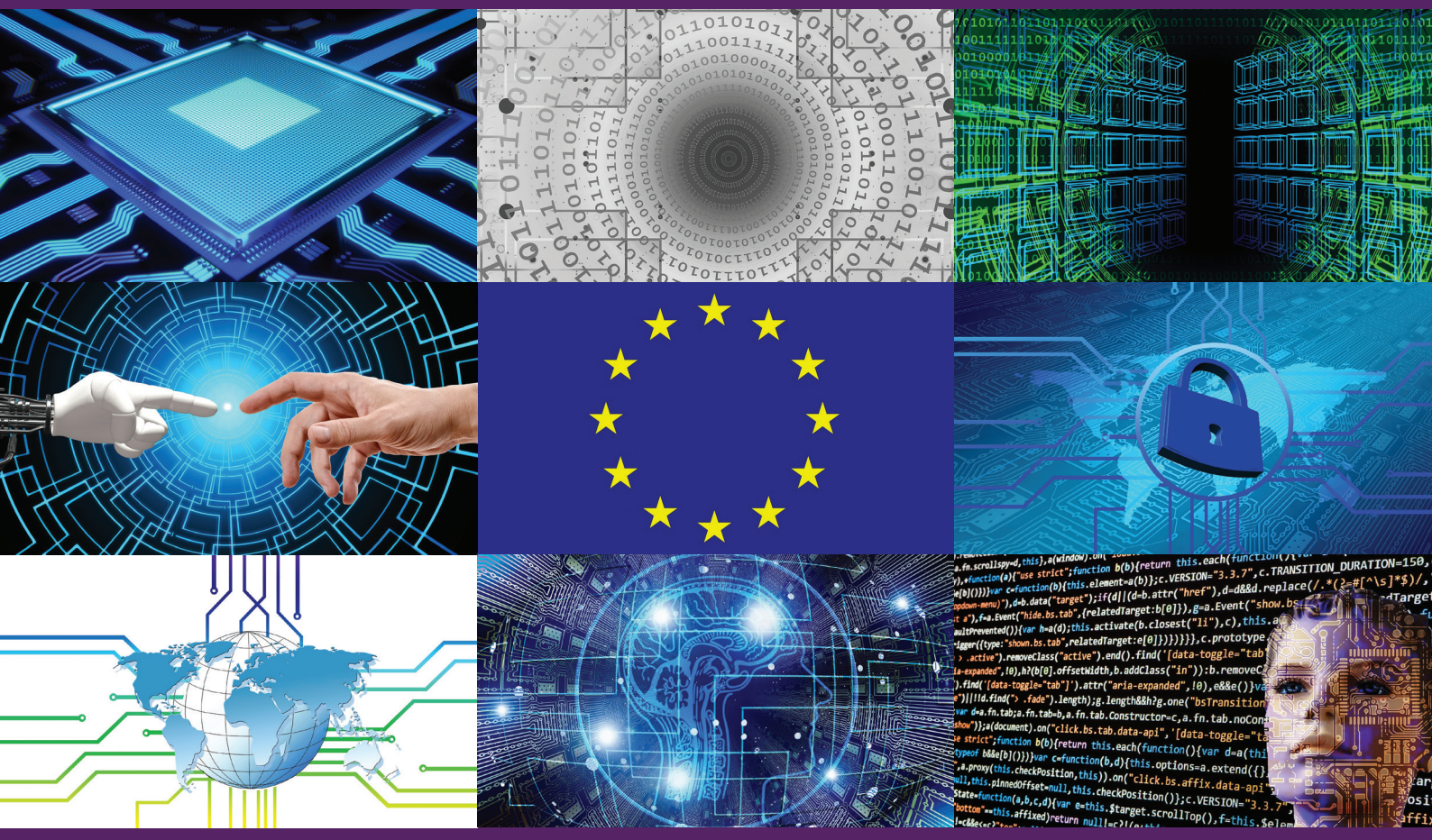
EUROPEAN REVIEW OF DIGITAL ADMINISTRATION & LAW

VOLUME 6
ISSUE 1
2025

LAW ENFORCEMENT TECHNOLOGIES: THE REALM OF FACIAL RECOGNITION



aracne

ERDAL

European Review of Digital Administration & Law / Erdal – *biannual review*

Submitting manuscripts
Manuscripts should be submitted via email to info@erdalreview.eu
For any queries on submission guidelines and procedures, please contact the Review.

Citation format
Editorial rules can be downloaded from the Review website.

Peer review procedure
This journal uses a double-blind review model.

Subscriptions
For subscriptions please contact: info@adiuvaresrl.it

Responsible Director: Angelo Giuseppe Orofino. Review registered at no. 12 of press register of the Court of Bari on 15 July 2020.

European Review of Digital Administration & Law

2025
Volume 6
Issue 1

ERDAL

This issue has been supported by four research projects:

The Metamorphoses of Public Law and the Transformations of Administrative Justice. Protecting Citizens in the Age of the Algorithmic Revolution, Climate Change, and Globalization, funded by LUM Giuseppe Degennaro University

PRIN: *Artificial Administrative Intelligence for territorial equality (2022KLAJ4P)*.

National Recovery and Resilience Plan, Mission 4 'Education and Research' – Component 2 'From Research to Business' – Investment 1.3, funded by the European Union – NextGenerationEU – CUP: F53C22000740007 – through the project titled *Cyber Social Security (CSS)*

Guía para la implementación de IA pública ética, confiable y al servicio del interés general: conciliar la innovación y el respeto a los derechos de las personas (Ref. FCT-24-19969), funded by Fundación Española para la Ciencia y la Tecnología - Ministerio de Ciencia, Innovación y Universidades.

ISBN
979-12-218-2111-6

Ist edition
September 2025

TABLE OF CONTENTS

Monographic Section: *Law Enforcement Technologies: The Realm of Facial Recognition*

(eds. Caroline Lequesne and Céline Castets-Renard)

European Review of Digital Administration & Law - Erdal
2025, Volume 6, Issue 1, pp. 69-77
ISSN 2724-5969 – ISBN 979-12-218-2111-6 – DOI 10.53136/9791221821116 08

*Facial Recognition Through the Lens of National Legislations - Italy**

Sveva Del Gatto
(Associate Professor of Administrative Law, Department of Law, University of Macerata)

ABSTRACT In recent years, facial recognition technology has spread rapidly in both the private and public sector: from detecting objects and people, to controlling access to public and private buildings; from group demographic analysis, to analysing emotions. In Italy, the use of facial recognition technologies is not widespread, but the examples that our legal system offers are significant for understanding the problems underlying the use of this software. Three cases of interest are highlighted: the use of facial recognition technologies in airports, the use of facial recognition technologies in stadiums, and the use of facial recognition technologies by the Police for investigation purposes. They show us that despite the great interest on the part of central and local public authorities, justified by the many benefits that facial recognition technology can bring, problems related to the high error rate, the risk of profiling without consent, bias and prejudice and the risk of violating people's fundamental rights and freedoms still remain unresolved. The solution adopted by the Italian legislator is in fact inadequate to face the new challenges posed by the use of facial recognition, particularly by public authorities, and on closer inspection it satisfies neither the expectations of those in favour of the use of these technologies in public places or places open to the public, nor those against. The Italian rule, specifically, appears short-sighted, not very courageous and not decisive.

KEYWORDS: Facial recognition technologies - Fundamental rights - Rule of law - Privacy - Data protection - AI Act

1. *Introduction*

This article examines the implementation of facial recognition technology (FRT) in Italy, focusing on use cases, regulations and future developments.

The first section looks at a number of projects and case studies. In particular, it reports on facial recognition at Milan airport, at the Olympic Stadium in Rome and the best-known case of SARI, Real Time and Enterprise, used by the Italian police.

The second section analyses the relevant Italian legislation, which is currently not very detailed, and the role played by the Italian Data Protection Authority (Garante per la potezione dei dati personali - GPDP) in setting the rules.

Finally, some considerations are made on future developments and unresolved issues.

2. *Facial recognition systems in Italy. The most significant case studies*

In recent years, facial recognition technology has spread rapidly in both the private and public sector:[1] from detecting objects and people, to controlling access to public and private buildings; from group demographic analysis, to analysing emotions. The face can be used to unlock smartphones, can be detected by CCTV cameras to enter offices, or to speed up e-boarding procedures in many airports. Facial recognition is known to be used for commercial purposes, e.g. to record the level of customer satisfaction, as part of emotive marketing, and also by Human resources offices for identifying, during a job interview, specific characteristics of a person with a view to hiring him/her.

*Article submitted to double-blind peer review.
The present work is included in the project "Innovation and Vulnerability. Legal issues and remedies" of the Department of Law, University of Macerata (funded by the Ministry of University and Research, programme Departments of Excellence 2023-2027).

[1] According to the study *The Global Expansion of AI Surveillance*, edited by the *Carnegie Endowment for Institutional Peace*, 43% of states (precisely 64 out of a reference sample of 176 states) used facial recognition technologies for surveillance purposes in 2019. East and Pacific Asia are the areas where there is - at least so far - the most widespread use of such technology (almost 70% of states use it), while in the Europe and Eurasia region less than 40% of countries have adopted facial recognition technologies for surveillance purposes. It is not only authoritarian systems that procure this kind of technology and invest in its implementation. The interesting fact that emerges from the Report is that it is precisely liberal democracies that are the main users of facial recognition technologies, with a deployment rate of 51% of the total sample, compared to the lower rate of 37% recorded in autocratic regimes. This means that one out of every two democratic states uses facial recognition devices for purposes - even in a broad sense - of surveillance.

Facial recognition is also widely used today by government authorities, who use these technologies to control access to public buildings,[2] to control access to airports or subways, for border control, to make digital public services more efficient, but also and above all for reasons of crime prevention and crime fighting.[3]

In Italy, the use of facial recognition technologies is not widespread, but the examples that our legal system offers are significant for understanding the problems underlying the use of this software. Three cases of interest are highlighted: the use of facial recognition technologies in airports, the use of facial recognition technologies in stadiums, and the use of facial recognition technologies by the Police for investigation purposes.

2.1. *Facial recognition technologies in Italian airports*

The first example of facial recognition is offered by the use of this technology in Italian airports, similar to what happens in other jurisdictions.[4]

The Face Boarding system is active at Milan Linate airport. Face Boarding allows travellers who have registered and expressly given their consent to reduce the time of document checks by making the boarding gates 'self-service'.[5]

The legal basis underlying this mechanism is precisely the explicit consent of the person concerned, which can only be given by persons of legal age.

The provisions on the use and processing of data contained in the Face Boarding Privacy Policy indicate compliance with the relevant regulations as dictated by the General Data Protection Regulation (GDPR):[6] the biometric data collected are not stored in readable form; in fact, encrypted templates are generated and then used only for the duration of the journey.[7] Finally, according to the information provided the data collected are not shared either with police databases or with other external databases.

Fiumicino Airport has also launched a trial involving the use of facial recognition to speed up checks and boarding (the 'youboard' project). Here too, according to the privacy policy,[8] participation is optional and consent

[2] In Italy, in Rome, at the entrance to Palazzo Chigi - the seat of government - nineteen thermoscanners for access control with thermographic detection were installed in 2020 for the containment of the Covid-19 pandemic, which also allow, however, the function of facial recognition, moreover using technology from Chinese companies.

[3] In transport, facial recognition tech is used for things like access control. In China, facial recognition systems are at bus stops and train entrances and scan passengers' faces instead of physical tickets or digital ticket codes. Similar uses are being tested in Kazakhstan. Facial recognition is in use, for example, at Madrid-Barajas, Barcelona and other airports operated by Aena. It is being used, in particular, to speed up security checks and boarding, as is the case with Air Europa and Iberia. In Italy, facial recognition systems and other biometric technologies are being implemented to optimise border controls, such as the FACE2FLY project in some airports. In the United States, US Customs and Border Protection uses facial recognition technology to screen people seeking admission to the United States.

[4] A report by 'Airports Council International World' points out that, globally, airports have accelerated their investments in technology to support recovery from the pandemic: 5.46 per cent of revenues were spent on IT in 2020, equivalent to about USD 3.5 billion in absolute spending, and 55 per cent of the airports surveyed estimated that their budgets would increase during 2021. Examples in Europe include the city of Madrid. Here, the airline Iberia, in collaboration with the Spanish airport authority Aena, the IT company Inetum and the biometric technology provider Thales, launched a biometric facial recognition trial during boarding at the Adolfo Suárez Madrid-Barajas airport. The initiative was also supported by the Centre for Industrial Technology Development, the Spanish Agency for the Development of Industrial Technology. In the testing phase - in Italy - facial recognition was used at the airports of Rome Fiumicino (the first, a few years ago, to have installed a system capable of cross-referencing passport scanning and passenger face scanning), Rome Ciampino and Milan Linate airport.

[5] The Face Boarding project was developed by SEA, a company operating at Milan airports. The biometric technology was first introduced at Linate in 2019, with the launch of a pilot programme aimed at testing the effectiveness and satisfaction of passengers. This experimental phase mainly involved passengers on specific flights, such as the Milan-Rome Fiumicino route and, subsequently, flights to Stockholm. Following the success of the pilot project, the system was extended to an increasing number of flights and passengers, making the technology available free of charge to all users and for all destinations covered by the airport. The go-live of the continuous solution took place in May 2024.

[6] Regulation (EU) No. 2016/679.

[7] As stated in the privacy policy, the data are only processed for the purpose of joining the service. In particular, facial images are not stored but are only used to create a biometric template required for access to security controls and, possibly, boarding gates. Personal data relating to the identity document, on the other hand, are stored - in encrypted form - for a period ranging from 24 hours after the flight actually takes off, to 31 December 2025, depending on the consent given by the passenger during registration. Finally, personal data from the boarding pass are automatically deleted 24 hours after the actual flight departure.

[8] Available at: www.adr.it/privacy-controllo-biometrico.

is the legal basis for data processing.

At present, facial recognition is not yet widespread in Italian airports. However, the two cases mentioned above, which concern the main national airports, suggest that this practice will become more widespread in the future.

2.2. *Facial recognition technologies in Italian stadium*

The second case study is that of the Olympic stadium in Rome.

Since 2016, a video surveillance system using facial recognition technology has been in use at the Olympic Stadium in Rome. It provides images of spectators that are automatically matched to the name of the person as recorded in the turnstile access control system and the ticketing system (the personal details of the purchaser are requested when tickets are issued for football matches). The Ministry of the Interior justified this decision on the grounds of a resurgence of violence during matches at the Olympic Stadium, explaining that although the existing video surveillance system provides a good overview of the flow of people and the stands inside the stadium, it is insufficient to identify individuals responsible for prohibited behaviour, so that effective technical means are necessary to fully identify those responsible for disturbances without putting the safety of police officers at risk.[9]

The technological systems in question comply with the provisions of the Decree of the Minister of the Interior of 6 June 2005 on video surveillance in sports facilities; the data and images are stored on servers installed in secure, protected areas at the Olympic Stadium and are not transmitted outside the stadium by electronic means; the data is accessed by police personnel for security or judicial police purposes, using technicians appointed by the companies which, on behalf of CONI, are responsible for the management and maintenance of the video surveillance technology. Data relating to images acquired and linked to names are automatically deleted after seven days, as is the case for data collected by all existing cameras.

The data controller is the Ministry of the Interior, in the person of the Rome Police Commissioner pro tempore. The data processor is a police officer appointed by the Rome Police Commissioner as coordinator of the Security Operations Group.

With reference to this system, the Data Protection Authority has expressed a positive opinion provided that the system is used directly and exclusively by police officers for the sole purpose of preventing, investigating and suppressing conduct for which access to places where sporting events are held is prohibited, or more serious crimes; the companies used by the system operator are designated as data processors, without prejudice to the fact that the natural persons who physically process the data, in particular those who access the system for maintenance operations, must be designated as data processors and must be given the necessary instructions; the logical protection of the images must be ensured by strong authentication mechanisms.[10]

In 2021, the video surveillance system with facial recognition underwent a change. The system used at the Olympic Stadium is called Reco Finder and allows automatic recognition of faces when they are found in a database of individuals with photos in order to pre-identify individuals subject to DASPO.[11] According to an investigation published by Wired,[12] given a series of photos of individuals subject to DASPO, the algorithm is able to analyse the video stream in real time and detect the presence of a wanted person, sending an alert to the authorities.

[9] The system is used for the offences provided for in Article 6 of Law No. 401/1989 and subsequent amendments.

[10] GPDP, 28 July 2016 n. 338, available at: www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5386852.

[11] Most of the offences relating to sport are contained in Law No. 401 of 13 December 1989, which regulates illegal gambling and betting and protects the integrity of sporting events. The most significant instrument, governed by Article 6 of the aforementioned Law No. 401 of 1989, is the Prohibition of Access to Sporting Events (D.A.SPO.), amended by Decree Law No. 8 of 8 February 2007, converted by Law No. 41 of 4 April 2007. The D.A.SPO. is an atypical preventive measure that prohibits individuals considered dangerous from accessing places where certain sporting events are held. In particular, the measure is applicable to individuals who have been reported or convicted in the last five years or who are in situations that indicate they are a threat to public order and safety. For such individuals, the police commissioner may prohibit access to venues where specific sporting events are taking place, as well as to areas where those participating in or attending such events are likely to stop, pass through or be transported.

[12] See www.wired.it/article/riconoscimento-facciale-stadio-olimpico-roma.

This is therefore a case of real-time facial recognition on which the Data Protection Authority has not yet ruled.[13]

2.3. *The use of facial recognition technologies by the Italian Police for investigation*

The latest case study related to the Italian system, undoubtedly the most interesting, is that of SARI (Sistema Automatico di Riconoscimento Facciale) used by the Italian State Police since 2018, as part of investigative and crime prevention activities. SARI makes it possible to compare the images taken by surveillance cameras with the images contained in the A.F.I.S. Database.[14] The system is able to operate in both Real Time and Enterprise modes. In the latter case, the operator uses SARI (Enterprise) to search for a match between the identity of a face (based on an image also acquired online) with other images already in a large database. To do so, facial recognition algorithms are used. Once the algorithm has been queried and the output has been acquired, the identification of the face that most closely matches the one under investigation is the task of the police officer. Human input is therefore indispensable.

In Real Time mode, the SARI system is instead designed to provide real-time results on 'live video' streams from cameras positioned in certain public areas of cities. The acquired data are then analysed and compared by means of a facial recognition algorithm with the data on a 'watch list' available to the public authorities.[15] When a match is detected, the system generates an alert. This function was conceived in particular to allow, during events and demonstrations, to reinforce the territorial control system.

3. *The regulatory context and the role of the Italian Data Protection Supervisor (GPDP)*

Despite the widespread and, as will be discussed, growing interest in the use of facial recognition technologies also by public authorities, Italy lacks specific legislation. Only in 2021, the so-called 'Decreto Capienze',[16] aimed at introducing provisions on the management of the Covid-19 pandemic emergency, introduced a temporary moratorium than banned the use of video surveillance equipment with facial recognition in public places or places open to the public.[17] The ban, subsequently extended until 31 December 2025[18] is, however, not absolute: processing operations carried out by the competent authorities for the purpose of preventing and suppressing criminal offences or enforcing criminal sanctions are excluded, provided that a favourable opinion of the Italian Data Protection Authority is obtained. However, the opinion is not needed if the processing is carried out by the judicial authority in the exercise of its judicial functions or by the public prosecutor .[19]

[13] See "Big Brother at the Olympic Stadium: who manages facial recognition data at Rome's stadium?" - HuffPost Italia, 24 February 2024.

[14] Acronym of Automated Fingerprint Identification System, or Automated Fingerprint Identification System AFIS allows the so-called 'minutiae', the characteristic points of each person's fingerprints, to be encoded and compared with the information contained in the Central Criminal Police Identity Records, in which all the photo-identification cards issued by Italian and foreign police forces are stored; within the archive are stored both the fingerprint images and the photographs and biometric data of all the subjects who are subjected to the detection.

[15] The images used for comparison are, as mentioned above, contained in the AFIS database (acronym for Automated Fingerprint Identification System). In the technical specifications, there are approximately 10 million images that can be used by artificial intelligence. However, some sources based on police statements indicate that the AFIS database contains well over 16 million images, the processing methods (collection, processing and storage) of which are not entirely known. One of the possible explanations put forward to explain the discrepancy between the data stated in the specifications and the data provided by the police is that SARI draws partially on the data contained in the EURODAC database (acronym for European Asylum Dactyloscopy), which contains the fingerprints of asylum seekers and irregular foreigners who are reported on European territory. However, the gap between the actual data and the declared data could be due to the massive acquisition of images online (as happened, for example, in the United States, which acquired millions of images from social media or websites), or to the inclusion in the database of data from the Reception Management System (SGA), used to identify migrants. For more information on this, please refer to the article available at: www.agendadigitale.eu /sicurezza/privacy/sari-vantaggi-e-rischi-del-riconoscimento-facciale-nella-pubblica-sicurezza.

[16] Decree-Law No. 139 of 8 October 2021 'Urgent provisions for access to cultural, sporting and recreational activities, as well as for the organisation of public administrations and the protection of personal data'.

[17] See article 9, Decree-Law No. 139 of 8 October 2021.

[18] The deadline initially set for 31 December 2021 was first shifted to 31 December 2023 and lastly postponed to the end of December 2025 by Article 8 of the 'Public Entities' Decree Law, 10 May No. 51.

[19] As established by Article 9, paragraph 12, the prohibition on the use of facial recognition systems in public places or places open to the public 'does not

The consultative activity of the GPDP, even before the entry into force of the aforementioned rule, has proved very useful in enucleating the principles that should guide public administrations when using facial recognition for purposes of public interest, such as security and public order. We also believe that it could be considered indicative of an evolving understanding of the issue of fundamental rights guarantees.

In addition to the already mentioned opinion of the GPDP on the Olympic Stadium in Rome, the opinions adopted on the use of SARI Enterprise and SARI Real Time are of great interest.

In the opinion issued on the SARI Real Time,[20] the Authority for data protection considered the instrument unlawful because it was used without an adequate legal basis.

In the view of the GPDP, the implementing decree of the Personal Data Protection Code on the processing of data for public security purposes by police bodies, offices and commands cannot be considered an adequate and sufficient legal basis.[21] The decree lacks the degree of detail required to meet the need for predictability that is essential when the police use real-time facial recognition technologies. In fact, it contains specific rules only for the processing of data collected through video surveillance and photographic, audio and video recording systems which, however, as noted by the Authority, are "ontologically different systems from those for processing biometric data".[22]

According to the GPDP, real time facial recognition "achieves large-scale automated processing that can also concern, *inter alia*, those present at political and social events, who are not the subject of 'attention' by the police". It is therefore determined, and this is the most interesting part of the opinion, "an evolution of the very nature of surveillance activity, moving from the targeted surveillance of certain individuals to the possibility of universal surveillance for the purpose of identifying certain individuals".[23] For this reason, a specific regulation setting out in detail the conditions and limits for the use of this form of video surveillance is strictly necessary. In its absence, SARI real time has been banned.[24]

In contrast, SARI Enterprise was considered by the Italian Data Protection Authority legally allowed because it does not carry out any additional processing compared to that previously carried out by the AFIS (Automated Fingerprint Identification System), but merely "automates certain operations that previously required the manual input of identifying features".[25] That is, SARI Enterprise allows the operations of searching the database of photo subjects by entering a photographic image, which will be automatically processed in order to provide the list of similar mug shots, obtained through a decision-making algorithm that specifies their priority.

The fundamental distinction between SARI Real time and SARI Enterprise, according to the argumentation of the Italian Authority, lies in the fact that SARI Enterprise does not represent a new processing operation, but only a *new processing method*. More precisely, it is a "mere aid to human action, with the aim of speeding up the identification, by the police operator, of a wanted person whose facial image is available, without prejudice to the need for the operator's intervention to verify the reliability of the results produced by the automated system".[26]

The two opinions by GPDP are not, however, in contradiction with each other. The opinions on SARI, Real time and Enterprise, although of opposite sign, are the result of a clear vision of the problem that distinguishes the cases in which artificial intelligence is in an instrumental function with respect to the final decision, adopted by the human being, from those in which it is the software that actually decides. Also, worth mentioning is

apply to processing carried out by competent authorities for the purposes of preventing and suppressing crime or enforcing criminal penalties referred to in Legislative Decree No. 51 of 18 May 2018, in the presence of the data subject, except in the case of processing carried out by judicial authorities in the exercise of their judicial functions and by the public prosecutor's office, with the favourable opinion of the Data Protection Authority.' 51, in the presence, except in the case of processing carried out by the judicial authority in the exercise of its judicial functions and those of the public prosecutor, of a favourable opinion of the Data Protection Authority issued pursuant to Article 24, paragraph 1, letter b), of the same Legislative Decree No. 51 of 2018'.

[20] Garante per la protezione dei dati personali (GPDP), Opinion No. 127 of 25 March 2021.

[21] *Idem.*

[22] *Idem.*

[23] *Idem*.

[24] According to the GPDP opinion referred to above (Opinion No. 127 of 25 March 2021).

[25] Garante per la protezione dei dati personali (GPDP), Order No. 440 of 26 July 2018.

[26] *Idem*.

the centrality accorded to the principle of rule of law. Due to the intrusiveness of facial recognition technologies, a legal basis that broadly regulates the use of audio and video footage is not sufficient. What is needed is a specific and detailed law limiting the discretion of administrative authorities in the use of facial recognition as a guarantee for the persons concerned.

If one compares the opinion on SARI Real Time with the one on the Olympic Stadium in Rome, a change in sensitivity on the issue is then evident (and the trend is confirmed by the new enquiries opened by the GPDP[27]): if the opinion on the Olympic Stadium in 2016 and prior to the entry into force of the GDPR is characterised by a broader openness,[28] the opinion on SARI Real Time confirms a greater awareness of the risks and problems associated with the use of facial recognition.

4. *Open projects, regulatory developments and unresolved knots*

Currently in Italy, the focus on the use of facial recognition software for deterrence, prevention and crime-fighting purposes, and therefore for reasons of security and public order, is very high.

In addition to the cases mentioned, from use in stadiums and airports to use by the Police, in many Italian cities, municipal resolutions have been adopted for the installation of video cameras with facial recognition functions.

The examples are numerous. In 2020, in order to ensure urban security and the decorum of the city, the municipality of Turin drew up the "Argo" project, which envisaged the installation of an intelligent video surveillance system.[29] The project was submitted to a procedure before the GPDP, but was not followed up: in fact, the City of Turin never sent the Italian Authority the documentation requested for the conclusion of the preliminary investigation phase.

Other attempts to install video cameras with facial recognition systems were made by the municipal administrations of the cities of Torino,[30] Como,[31] Lecce,[32] Arezzo[33] and Rome.[34] In all these cases, the GPDP initiated proceedings. The Italian Authority pointed out, in particular that under European and national law the processing of personal data carried out by public entities, by means of video devices, is generally allowed if necessary for the performance of a task conducted in the public interest or in connection with the exercise of public powers.[35] However, in the case of municipalities, the use of video-surveillance systems is only possible on condition that a "pact for urban security between the Mayor and the Prefecture"[36] is stipulated, but which does not always exist in the cases referred to. The Authority also recalled how "until a specific law on the subject comes into force, the installation and use of facial recognition systems using biometric data are not allowed in Italy, unless the processing is carried out for judicial investigations or crime prevention and repression". In fact, it is necessary for the Parliament to define admissibility requirements, conditions and guarantees, establishing which uses of these technologies are desirable and in what terms it is possible to limit the rights at stake due to higher public needs.

Despite the great interest on the part of central and local public authorities, justified by the many benefits that facial recognition technology can bring, problems related to the high error rate,[37] the risk of profiling without

[27] See next paragraph.

[28] It is also the subject of criticism according to which the GPDP should intervene again on this point.

[29] In agreement with the local police and the public company 5T, this project envisages the installation of 273 cameras on the streets of Turin - in addition to the 107 already present in the main city locations for the control of mobility and traffic - at a cost of more than two million euro. Their main functions relate to detecting the crossing of a line, intrusions into an area, and the entry or exit of someone or something in a given area. It is envisaged that by means of special algorithms the data collected will be recognised, extracted and analysed, then anonymised and entered into a single central system, which is made available to the local police and the police forces to combat crime, especially in the peripheral and most degraded areas of the city. See Municipal Council Resolution No. 1738/048 of 4 August 2020.

[30] For more information see www.garanteprivacy.it /home/docweb/-/docweb-display/docweb/10035760.

[31] For more information see www.garanteprivacy.it /home/docweb/-/docweb-display/docweb/9591331.

[32] For more information see www.garanteprivacy.it /home/docweb/-/docweb-display/docweb/9823282.

[33] *Idem.*

[34] See the GPDP communication on the website www. garanteprivacy.it/home/docweb/-/docweb-display/docw eb/10012392.

[35] GPDP, Provision of 22 February 2024 no. 105

[36] See the GPDP communication available at www.gara nteprivacy.it/home/docweb/-/docweb-display/docweb/9 823282.

[37] In this regard, it is positively reported that the Italian

consent,[38] bias and prejudice[39] and the risk of violating people's fundamental rights and freedoms[40] remain unresolved.

The solution adopted by the Italian legislator is in fact inadequate to face the new challenges posed by the use of facial recognition, particularly by public authorities, and on closer inspection it satisfies neither the expectations of those in favour of the use of these technologies in public places or places open to the public, nor those against. The Italian rule, specifically, appears short-sighted, not very courageous and not decisive.

Not very courageous and short-sighted because it considers neither the inevitable technological advances nor the actual needs of citizens to be able to take advantage of the benefits made available by facial recognition technologies. New technologies offer enormous opportunities for better protection of public interests, such as ensuring greater security and more effective public order. Banning the use of new technologies out of fear (albeit real) that they may undermine fundamental rights does not seem to me to be the best way forward. On the contrary, strict regulation allowing their use within precise limits and under certain conditions is to be preferred.

Not very decisive, from the perspective of protecting fundamental rights, because the ban introduced is subject to broad limits. A targeted legislative intervention would have been preferable, rather than a rule inserted in a decree intended to regulate other issues. A specific and detailed law was needed to set limits and assumptions and to introduce adequate safeguards for persons whose biometric data are processed, first and foremost with the provision of stringent transparency obligations, *ex ante* and *ex post*[41] as, moreover, pointed out by the Italian Data Protection Authority.

Instead, the Italian legislator's choice appears to have been a solution of convenience pending the final approval of the AI Act and its entry into force, which finally took place in May 2024, after a tortuous legislative process.[42] The Artificial Intelligence Regulation itself, however, leaves one somewhat dissatisfied. There are lights and shadows in it. To be welcomed is the introduction, for the first time, of an *ad hoc* discipline for facial recognition technologies and processing of biometric data. The decision to introduce an articulation of protections that concerns both the moment of production of these technologies and their release onto the market, and also that of their operation[43] is to

Police commissioned a group of researchers to carry out some experiments in order to verify when facial recognition for the detection of a suspect is most effective and when it has high error rates. The preliminary results of this study can be consulted in the work by P. Contardo, P. Sernani, S. Tomassini, N. Falcionelli, P. Castellini and A.F. Dragoni, *FRMDB: Face Recognition Using Multiple Points of View*, in *Sensors*, 2023, 23(4), 1939, https://doi.org/10.3390/s23041939.

[38] B. Davidow, *Welcome to Algorithmic Prison. The use of Big Data to profile citizens is subtly, silently constraining freedom*, The Atlantic (Washington, DC), 14 February 2014.

[39] An interesting example of how biases can invalidate the results of an algorithmic system comes from the well-known COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) case, a system designed to quantify the risk of recidivism of individuals undergoing criminal proceedings, produced by a commercial company, and used in multiple US jurisdictions to calculate the likelihood of committing further offences over the next two years, and to decide the type and amount of punishment to be imposed, as well as the manner in which it should be carried out. Scholars verified, by analysing more than 10,000 criminal defendants in Broward County, Florida, and comparing their expected recidivism rates with the rate that actually occurred over a two-year period, that black defendants were much more likely than white defendants to be wrongly convicted at a higher risk of reoffending. The study is reported in J. Larson, S. Mattu, L. Kirchner, J. Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, 23 May 2016, www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. See also S. Barocas and A.D. Selbst, *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, No. 3, June 2016, 671 ff.

[40] P. Alston, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/74/493 of 11 October 2019, available at: https://undocs.org/A/74/493.

[41] On transparency as a necessary safeguard of the rule of law transparency and the rule of law by legal philosopher M. Hildebrandt. See M. Hildebrandt, *The Issue of Bias. The Framing Powers of Ml*, in M. Pelillo and T. Scantamburlo (eds.), *Machine Learning and Society: Impact, Trust, Transparency*, MIT Press, 2020, available at: https://ssrn.com/abstract=3497597 or http://dx.doi.org/10.2139/ssrn.3497597. And earlier, already, EAD., *The Dawn of a Critical Transparency Right for the Profiling Era*, *Amsterdam Digital Enlightenment Yearbook*, 2012. On the role of transparency as a key component of an effective accountability system C. Zimmermann and J. Cabinakova, *A Conceptualisation of Accountability as a Privacy Principle*, in W. Abramowicz (ed.), *Business Information Systems Workshops, Lecture Notes in Business Information Processing*, vol. 228, Cham, Springer, 2015.

[42] Regulation (EU) No. 2024/1689 of the European Parliament and the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

[43] The use of real-time biometric identification in publicly accessible spaces for law enforcement purposes

be welcomed. Together with the GDPR, the regulation therefore offers a legal basis that is suitable for precluding the arbitrary use of biometric devices. However, there is no shortage of critical points that mitigate, to a certain extent, the revolutionary scope of the Regulation.[44] The wide range of offences that justify the adoption of real-time facial recognition systems is not fully convincing, as well as the fact that the prohibition of the latter has been limited to law enforcement activities in spaces accessible to the public, thus making the hypotheses not covered under the GDPR fall under the GDPR with the emergence of not a few problems. Owing to the 'weak' limitations of facial recognition *a posteriori*, the risk presented is that of biometric technologies being used for purposes other than those envisaged. In any case, the question remains unresolved of the provision of an internal regulation specifying assumptions and, above all, limits and guarantees of the use of these technologies by public administrations in cases where, in compliance with the AI Act, their use is permitted. With regard to the procedural safeguards to be put in place to protect citizens against the use of facial recognition (and artificial intelligence software in general) by public administrations, some guidelines that the legislator should follow come from the Italian administrative court.[45] Others guarantees can be found in the judgments of courts in other jurisdictions.[46] In all these judgments, the role of principles such as rule of law, proportionality and transparency is critical. Thus, the centrality of administrative law as a rule of balance and guarantee between (digital) authority and fundamental freedoms and as a source of protection for new rights is confirmed.

Alongside the passing of a law on the subject, which would be very useful and mandatory, it would also increase transparency for the benefit of the public[47] and the successful use of facial recognition technologies. On the functioning of SARI, for instance, there is very little data available on the number of searches performed and the number of searches that have produced operational results useful for investigations.[48] There is also a lack of up-to-date information on the accuracy of the data collected by the algorithms on which the software operates, or

is listed as a prohibited practice in Article 5. However, three exceptions are provided for in Article 5(1)(h), which allow its use when strictly necessary and for the sole purpose of confirming the identity of a specific person. As for ex post biometric identification systems, they have instead been included among high-risk practices: their use is therefore not prohibited, but a link with a crime, criminal proceedings, a real and present or actual and foreseeable threat of a crime or the search for a specific missing person must be proven, in addition to the necessary provision of transparency measures and the obligation for deployers to obtain authorisation from the competent authorities (Article 26(10)).

[44] Already highlighted in the first comments on the draft regulation. See C. Casonato and B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, n. 3, 2021.

[45] Consiglio di Stato Sez. VI, 13 December 2019, n. 8472. See www.irpa.eu/focus-sentenze-g-a-su-decisioni-algoritmiche-consiglio-di-stato-sentenza-n-2270-del-2019-come-incoraggiare-lutilizzo-di-algoritmi-nei-procedimenti-amministrativi-senza-dimentic.

[46] Although still limited in number, and not always specific to facial recognition but referable to other artificial intelligence systems. In Italy, see for example, Consiglio di Stato, 8 April 2019, No. 2270; See Royal Courts of Justice Strand, London, WC2A 2LL Date: 11/08/2020, available online at www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. As noted by the English courts of second instance: 'the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law'.

[47] The opacity on the functioning and purposes of the adoption of the applications under examination is common to the various experiences recalled in this paper. It is seldom possible to find precise indications as to the modalities by which they operate: in the cases analysed, generic reference is made to the control of entry gates, but it is not always clear whether one is talking about authentication or identification, or monitoring that takes place in real time or ex post. Similarly, confusion is demonstrated by the overlapping of multiple purposes, including prevention, security, access management, combating racism and discrimination, and the detection of offenders and recipients of access prevention measures. Given the difficulty of distinguishing between concepts such as 'authentication' and 'identification', possible users of facial recognition systems need to try to define the activities they are carrying out, because the configuration of the aspects listed has several implications, both in terms of rights and freedoms and in terms of the legal instruments that can be activated to protect them. citizens should be able to foresee and control the potential uses of their personal data. This becomes complex in the era of *big data*, with algorithms designed for self-learning and adaptation, but based on human judgements or biases embedded in their creation. See A. Turing, *How can we design fair, transparent, and accountable AI and robotics?*, Alan Turing Institute, 2014.

[48] The last publication dates back to 2016 (thus before the adoption of the system by the forensic police). To date, according to the agents, 'there is no minimum percentage of similarity from which the result is considered reliable, but the list of candidates is always reviewed manually by a specialised operator'.

on the type of crimes for which facial recognition can be used. Greater transparency, on the other hand, would reduce (though not eliminate) the risk of privacy violations and the possibility of abuse such as the collection and storage of sensitive data, the possibility of misidentification or the use of these technologies for mass surveillance. For instance, it could be very beneficial to regularly initiate impact assessments of biometric processing under Article 35 GDPR. Such assessments should take into account the error rates recorded in the experiments carried out and the consequences for the rights and freedoms of the persons concerned, as now required by the AIA.[49] Information relating to the composition of the databases consulted should be made accessible to the persons subject to profiling, as also provided for in Articles 10, 11, 12 and 13 of the AIA. Information about the composition of the databases consulted should be made accessible to the persons being profiled, as also provided for in Articles 10, 11, 12 and 13 of the AIA, in order to make artificial intelligence truly trustworthy,[50] as requested in the European Commission's White Paper on AI.[51]

[49] See article 27 AIA. One of the most important new features of the AIA is the assessment of the impact on fundamental rights, which aims to evaluate the impact of AI systems considered to be high risk on fundamental rights. The impact assessment for AI should focus not only on personal data, but more generally on fundamental rights, such as human dignity and integrity, individual freedom, equality and solidarity, justice, democracy, the rule of law and the environment. In the case of FRIA, the impact assessment is also carried out at an early stage, before an AI system is placed on the market or used in critical contexts (*e.g.* facial recognition, predictive analysis in the criminal field, etc.).

[50] An interesting best practice is that of public registers on artificial intelligence systems used by public administrations introduced in some northern European cities. For instance, the cities of Amsterdam and Helsinky have set up a '*Public AI Register*' as *'a window into the artificial intelligence systems used by a government organisation*'. Transparency registers are intended to enable government organisations to satisfy citizens' queries on the functioning of algorithmic systems; to help document (in a standardised, searchable and archivable manner) the decisions and assumptions that have been made in the process of developing, implementing, managing and finally decommissioning an algorithm; or, finally, to provide information that helps people 'familiarise' themselves with government AI systems. In essence, through the introduction and implementation of these registers, the aim is to involve citizens more by providing them with knowledge of the algorithms in use in administrations in order to ensure '*transparency, accountability and explicability*'. On the importance of ensuring transparency on the part of public administrations when they make use of artificial intelligence algorithms, see S. Del Gatto, *Potere algoritmico, digital welfare state e garanzie per gli interessati. I nodi ancora da sciogliere*, in *Rivista Italiana Diritto Pubblico Comunitar*io, 6, 2020, 829 ff.

[51] European Commission, *White Paper on Artificial Intelligence: a European Approach to Excellence and Trust*, 19 February 2020.