

MAPPING THE USE OF FACIAL RECOGNITION TECHNOLOGIES IN ITALY

A research on the practices of Police Headquarters,
Public Prosecutors' Offices and Municipalities



The Research-Phase 2 was conducted for StraLi by: **Lorenzo Sottile**
With the contribution to the data collection of: **Fabio Gaggero**

Reviewers: **Alice Giannini, Serena Zanirato**
Graphics & media: **Greta Temporin**

The research is [funded](#) by the Digital Freedom Fund as part of their pre-litigation research support.



The information contained in this report is updated until 1/9/202



Table of contents

1. Introduction	4
2. Methodology	7
3. The first issue encountered. The lack of replies from the Police Headquarters and the Public Prosecutor's Offices	10
4. The position of Municipalities on facial recognition technologies before, during, and after the moratorium	12
4.1 Before the moratorium	17
4.2 During the moratorium	20
4.3 After the moratorium	23
4.4 Funds and partnerships	24
5. Conclusions	27



1 Introduction

StraLi is an NGO founded in Italy in 2018 by lawyers and legal practitioners aiming to react to the inequities of the law and violations of human rights by putting their skills and abilities at the service of society. The association promotes the practice of Strategic Litigation and the respect of human rights through technical-judicial support given. StraLi obtained a pre-litigation research support grant from Digital Freedom Fund in order to answer the following research question: *what is the most strategic path to challenge the use of facial recognition technologies (“FRTs”) by law enforcement and judicial authorities in Italy?*

The first Report published by StraLi aimed at compiling the state of the art of the relevant legal framework. It presents jurisprudence on the impact that the use of facial recognition technologies (“FRTs”) by law enforcement and judicial authorities has on fundamental rights both at the Italian and European level¹.

In this second Report, StraLi has decided to develop new approaches to map the *effective* use of FRTs by different stakeholders in Italy. Specifically, the focus of our attention has been their adoption in particularly “critical” activities such as law enforcement and public spaces monitoring. For this reason, we decided to direct the investigation towards Police Headquarters, Public Prosecutors’ Offices, and Municipalities.

The possibility of using FRTs both in “*post*” remote mode and in real time by the aforementioned public authorities potentially poses a plurality of risks to the constitutional architecture of democratic States, thus questioning the endurance of an extensive catalogue of fundamental rights and freedoms. The reference is, *inter alia*, to the rights to the protection of personal data, respect for private life, non-discrimination, a fair trial. However, as pointed out in StraLi’s first Report, the *dissuasive* force of technologies, capable of generating the so-called “chilling effect”, should not be underestimated, as it might lead individuals to not exercise constitutional rights and freedoms, such as freedoms of expression, assembly and association².

¹ The first Report “*Building a litigation strategy to challenge the use of facial recognition technologies by law enforcement and judicial authorities in Italy*” is available [here](#). The Executive summary is available [here](#).

² See for example the EU FRA paper, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (November 2019).



The risks are even more evident if one takes into consideration that in Italy and Europe no specific legislation governing the use of these technologies is in place yet.

The legal framework, as well as the (institutional) positions on the matter, are ever-evolving. Pending the approval of the Regulation on Artificial Intelligence (so-called “AI Act”), important steps have been taken by the European Parliament (“EP”) during the adoption of its negotiating position on the Act on 14 June 2023, when the Act has been amended considerably from its original wording. Most notably, the list of AI systems prohibited in the EU has been remarkably changed to include now “post” remote uses of biometric technologies (in addition to real time biometric surveillance), with the only exception of its use for the prosecution of serious crimes³, and only after judicial authorisation. The EP also insisted on the ban of all biometric categorisation systems using sensitive characteristics, predictive policing systems, emotion recognition systems, and AI systems using indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases.

While the position of the EP can be positively welcomed, it is not the final EU position, as EU Member States in the Council are still in the process of the negotiations of the final text of the Regulation, with the aim to reach an agreement by the end of 2023.

When it comes to the Italian legal framework on the matter, the first Report extensively addressed the so-called moratorium on the installation and use of video surveillance cameras with FR systems in public places by public authorities or private sectors introduced by Italy through Decree Law no. 139/2021, converted into Law no. 205/2021 (Art. 9 (9)) in force until 31 December 2023⁴. The moratorium has been extended until 31 December 2025 by Law no. 87/2023 on 3 July 2023⁵.

The extension of the moratorium, however, was intended as a remedy to temporarily fill the existing legal vacuum. As pointed out by the Italian Data Protection Authority (DPA) in numerous instances, there is no legal basis at the national level that allows the *live* processing of biometric data extracted from individuals’ faces. Moreover, the DPA added that such a legal basis must appropriately foresee the use of these systems, after assessing all the rights and freedoms involved, without giving those who will be required to dispose of

³ It must be underlined that the idea of strictly identifying the hypothesis of a serious crime has not been taken into consideration.

⁴ Italy has followed the call of the European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters ([here](#)).

⁵ Conversion of [Decree Law no. 51/2023](#) containing urgent provisions on the administration of public bodies, legislative deadlines and social solidarity initiatives. Its Art. 8-ter replaced the words “31 December 2023” with “31 December 2025”.



it such a broad degree of discretion⁶. Despite the moratorium in place, some Municipalities, such as Lecce and Udine, expressly (and publicly) stated their intentions to implement video surveillance cameras equipped with FR systems as soon as possible, requiring the immediate intervention of the DPA to stop these attempts⁷. Similarly, the Minister of Interior Matteo Piantedosi has repeatedly showed some favour for FRTs by alluding to the extraordinary possibilities offered by FR in terms of prevention and detection of criminals in public spaces⁸.

In this context, despite the DPA's firm position, had the moratorium not been extended, there would have been an increased risk of opening up of the possibilities for the use of FRTs in Municipalities from 1 January 2024 onwards.

Furthermore, as extensively analysed within the first Report, the moratorium provides for some significant exceptions, whereby FRTs can still be used by "competent authorities" to prevent and repress crimes or execute criminal sanctions, in the presence of a favourable opinion of the DPA, and by the judicial authority in the exercise of judicial functions as well as judicial functions of the public prosecutor, even without the pre-emptive control of the DPA (article 9 (12) of the Law no. 205/2021).

The intention of some Municipalities to take advantage of the benefits offered by FRTs in terms of urban security, together with such broad exceptions to the moratorium and the DPA's positive opinion on the use of SARI-Enterprise⁹, were determining factors for the outset of the research.

This Report aims to shed light on past and present uses of FRTs, as well future intentions to deploy such technologies, through the creation of a map that involves the stakeholders that have attempted or are allowed to use FRTs in Italy: Police Headquarters, Public Prosecutors' Offices and Municipalities. In a framework of a lack of official information on how and when FRTs are used, there are serious risks of misuse of these tools and of negative impact on individuals' fundamental rights and freedoms.

⁶ See 2.3.1 and 2.4 [Research Report 1](#).

⁷ See in particular 2.5.1. of the [Research Report 1](#).

⁸ Alessandro Farruggia, "Il ministro Piantedosi: "Più polizia nelle stazioni. E bisogna sbloccare il riconoscimento facciale", *Quotidiano Nazionale*, 30 aprile 2023. Available [here](#); Fausto Carioti, "Seimila agenti in più per avere città sicure", *Libero*, 15 maggio 2023. Available [here](#).

⁹ In 2.3.2 of the [Research Report 1](#) we explained how SARI-Enterprise works.



2. Methodology

The investigation was carried out from 1st March to 31st May 2023, before the extension of the moratorium. However, such extension does not change the relevance of the research's outcomes, because we had generically investigated planning for the future by referring to the time when the moratorium expires. For instance, the period before the moratorium was in place, the period of the moratorium and screened future intentions have been under analysis in order to find out:

- A. The specific (public) authorities that are allowed to use or have used FRTs;
- B. How often the aforementioned authorities use (or have used) FRTs;
- C. Under what circumstances and for what purpose FRTs have been (or are supposed to be) used.

The research consisted of several phases:

I. Choice of the target

We decided to focus the research on three different stakeholders: Municipalities, Police Headquarters (Questure), and Public Prosecutor's Offices (Procure). The choice was made based on the fact that they were the best targets for obtaining answers to the main questions.

The rationale behind this selection is twofold:

Firstly, these entities represent the authorities with the capacity to employ Facial Recognition Technologies (FRTs) or, more broadly, the parties with the greatest vested interest in their utilisation.

Secondly, it is precisely this specific utilisation that has the potential to pose significant risks to the numerous fundamental rights and freedoms at stake.

II. Choice of the methodology: questionnaires as a research tool

The aim was to identify the most useful tool through which we could obtain the most (and most accurate) information possible.

The initial assumption was to resort to FOIA requests. However, we evaluated that there would be little practical possibility of obtaining information on FRTs from Public



Administrations (“PAs”) - especially within a short time frame. In fact, PAs might deny access to data and documents if it is necessary to avoid compromising public interests as public security and public order, national security, investigation and prosecution of criminal offences and proper conduct of inspection activities, among others¹⁰. For these reasons we discarded the tool and decided to proceed through questionnaires.

Secondly, the possibility of exercising the right to access by the data subject, provided by both Articles 14 of the Regulation 679/2016 (“GDPR”)¹¹ and 15 of the Directive 680/2016 (“LED”)¹² was considered. Nonetheless, this solution appeared rather unfeasible, as it relies on the direct awareness and cooperation of individuals who are under investigation, accused, or convicted and whose data has been subjected to processing via FRTs.

Eventually, the submission of informal and general questionnaires has been identified as a more useful and efficient tool. Consequently, the specific targets of the questionnaire, in order to narrow the recipients, were then selected. This has allowed us to send out the questionnaires and collect data in a more efficient way.

III. Sampling strategy:

- i. As far as Municipalities are concerned, we sampled all the county towns (*Capoluoghi di Provincia*)¹³ and 100 Municipalities. The municipalities selected were those that received most funds by the Ministry of Interior for the implementation of video surveillance systems according to a 2022 ranking of the Evaluation Commission of the Ministry of the Interior¹⁴. The selection was

¹⁰ Art. 5 bis (1) of Legislative Decree no. 33/2013, as amended by the Legislative Decree no. 97/2016.

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

¹³ They are the seats of the authorities in charge of an administrative district. A list can be found [here](#).

¹⁴ This ranking, available [here](#), is elaborated by the Evaluation Commission of the Ministry of the Interior on the basis of requests made by Municipalities for the installation of video surveillance systems, in accordance with criteria defined by the Minister of the Interior, in agreement with the Minister of Economy and Finance. In the context of the allocation of resources provided for by Article 35 quinquies of Law no. 132/2018, it can be noted how the expense authorisation related to video surveillance is increased year by year, adding to the €15 million in 2018 and 2019, €17 million in 2020, €27 million in 2021 and €36 million in 2022.

It is also relevant to emphasise that among the eligibility requirements of the applications of municipalities interested in the funding provided by Article 35 quinquies of Law No. 132/2018 - as specified by the [Decree of 27 May 2020 of the Ministry of the Interior](#) - is the implementation of video surveillance systems that do not



based on the close connection between surveillance cameras and FRTs. The questionnaires were therefore sent to the Public Relations Office and to the Data Protection Officer of each selected Municipality.

- ii. The form was also sent to Police Headquarters (*Questure*) and Public Prosecutor's Offices (*Procure*), respectively, to all the Italian Police Headquarters listed on the official website of the *Polizia di Stato*¹⁵; as well as to the Public Prosecutor's Offices of the regional capitals (*Capoluoghi di Regione*), both at the first instance Court (*Tribunale*) and at the Court of Appeal.

After determining the sample, we proceed to:

- IV. Collect recipients' email addresses;
- V. Draft the project presentation and the questionnaires;
- VI. Send out questionnaires and weekly reminders;
- VII. Collect the data;
- VIII. Process the data.

overlap with those already implemented in the last five years. This reference allows us to understand the importance recognised by the State to the increasing diffusion of these systems.

¹⁵ Available [here](#).



3. The first issue encountered. The lack of replies from the Police Headquarters and the Public Prosecutor's Offices

The decision to contact the Police Headquarters and Public Prosecutor's Offices was driven by three key factors:

1. the favourable opinion of the DPA on the use of the FR “post” remote system SARI-Enterprise by law enforcement authorities¹⁶;
2. the exceptions to the moratorium, which allow for the use of FRTs when employed by “competent authorities” for the purposes of crime prevention, law enforcement, and criminal sanctions execution.
3. the preliminary market consultation of the Department of Public Security in 2020 to enhance the functionalities of the two SARI components (Enterprise and Real-Time), together with the constant interest of law enforcement authorities in purchasing FR systems, as shown by the calls for tenders published by the Carabinieri and Guardia di Finanza in 2021¹⁷.

The main challenge driving this research has been **the lack of information about the functioning and performance of SARI-Enterprise**, despite its operation over the last 5 years. No knowledge of the “training” that the system undergoes is available; nor there is public disclosure about the error rates that characterise the algorithms and their potential discriminatory effects. Similarly, information on how many times SARI-Enterprise has been used and for which underlying offences is not available.

In other words, **there is currently no information that would indicate the precision of this tool nor its use is actually needed**. It is therefore even more challenging to evaluate whether its use is compatible with fundamental rights.

In order to shed light on these issues, the questionnaire submitted contained the following questions:

- A. Are you equipped with facial recognition technologies? If yes, please indicate briefly which ones
- B. Did you use facial recognition technologies? If yes, please indicate briefly which ones

¹⁶ [Provision no. 440 on 26 July 2018](#).

¹⁷ See 2.3.1. of the [Research Report 1](#).



- C. Through what procedure is the use of facial recognition technologies authorised?
- D. By whom is the use of facial recognition technologies authorised?
- E. How many times have you used facial recognition technologies since 2018? Only once; 2 to 10 times; 10 to 20 times; 20 to 50 times; 50 to 100 times; more than 100 times
- F. For which types of crimes have facial recognition technologies been used?
- G. Was the opinion of the DPA sought before the use of facial recognition technologies?

Regarding the Police Headquarters, we submitted the questionnaires to 106 offices. According to the standard procedure, the *Polizia di Stato* External Relations Department should have been contacted in advance to authorise the territorial Police Headquarters to answer the questionnaire. We emailed the Department, communicated with them via telephone and they told us that the matter was being processed.

Regrettably, as of the present date, we have not received any responses. This leads us to infer a strong inclination towards maintaining a low level of transparency on this subject.

Unfortunately, we achieved similar results when sending the questionnaires to Public Prosecutors' Offices. Only five out of 40 identified replied (Public Prosecutor's Office attached to the Court of Perugia, Roma, and Trieste and to the Courts of Appeal of Genova and Potenza), stating that they did not have FR systems in place and that they had never used them in their investigative activities.



4. The position of Municipalities on facial recognition technologies before, during, and after the moratorium

The research necessarily focused on Municipalities as well, due to their interest in surveillance technologies, especially video cameras, as demonstrated by their rapid spread within cities since the late 1990s and early 2000s¹⁸. These technologies played an important role in pursuing different purposes, including security, protection of heritage, control of specific areas and monitoring of traffic or vehicle access in historical centres, even in the absence of a specific legislation on video surveillance.

Considering the Italian lawmaker's inactivity on the matter, a key role was (again!) played by the Italian DPA. Apropos, the *Garante* tried to balance the interests pursued in the domain of public security (such as crime prevention) with the right to privacy of data subjects.

Of particular significance are the initial opinions issued by the DPA towards the Municipalities of Milano and Romano di Lombardia, respectively, in 1997 and 1998. In these opinions, the DPA highlighted that there was no necessity for clear and unequivocal identification of individuals through video surveillance. It sufficed that individuals could be identified through other means, such as cross-referencing with other sources of information like mug shots, identikits, or police archives containing images. Furthermore, the use of video surveillance systems without an elaborate system of safeguards raised numerous concerns, especially concerning the retention of images, the identification of individuals authorised to access the recordings, and the potential sharing of these recordings with third parties¹⁹.

In the newsletter of 28 February-5 March 2000²⁰ and in another intervention²¹, the DPA reiterated that local authorities that wanted to install video surveillance systems would have to comply with the principles set out in Law no. 675/1996 (Protection of persons and other subjects with regard to the processing of personal data)²². The DPA further stipulated the

¹⁸ G.G. Nobili, *L'occhio sulla città. La videosorveglianza nelle politiche locali per la sicurezza*, Quaderni C!VIVO, 2008, 11; A.P. Paliotta, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, Sinappsi, X, n.2, 2020, 109 et seq.

¹⁹ Read the DPA's opinions "Video surveillance - Installation by the municipality of Milan of several cameras in public places - 17 December 1997 [39849]" [here](#) and "Video surveillance - Installation of several cameras by a municipality - 28 May 1998 [1002044]" [here](#).

²⁰ Available [here](#).

²¹ Read "Video-surveillance - City of Mantova - Tele-surveillance project - 7 March 2000 [30987]" [here](#).

²² The Law transposed the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement



necessity of adopting various precautionary measures. These measures included, notably, restrictions on the magnification of the recorded footage and limitations on the level of detail concerning the physical characteristics of individuals captured by the video cameras.

The DPA has always paid particular attention to the compatibility of the installation and use of CCTV systems with individuals' fundamental rights, as demonstrated by the Decalogue of rules not to violate privacy of 29 November 2000²³ and the General Provisions on video surveillance of 29 April 2004 and 8 April 2010²⁴. The latter measure is of particular importance as it follows the adoption of the Law Decree no. 11/2009²⁵. Its Article 6 (7) provides the possibility for Municipalities to use video surveillance systems in public places or places open to the public to safeguard the urban security. However, Article 6 (8) sets out the limitation to seven days of the storage of data, information and images collected - with the exemption of special needs. These provisions have led to the standardisation of the use of video surveillance by Municipalities throughout Italy to intervene on security-related issues.

Currently, **FRTs represent the forefront of city surveillance**. They raise significant concerns and pose numerous risks to fundamental rights and freedoms, surpassing those associated with CCTV cameras. Gone are the days when zooming in or adjusting viewing angles were critical aspects of surveillance. FRTs operate by extracting distinct facial points, known as "fiduciary points", and comparing them with images in a database to identify potential matches. Municipalities are increasingly interested in these technologies for monitoring public spaces and conducting identification tasks aimed at the prevention and repression of crimes. Their potential is further enhanced through collaboration with various law enforcement agencies.

Thus, it is clear how FRT can be used by Municipalities to "urban safety". Urban safety is a slippery concept, which is defined by Article 4 of Decree-Law no. 14/2017²⁶ as "the public good that pertains to the livability and decorum of cities, to be pursued also through urban, social and cultural redevelopment, recovery of degraded areas or sites, the elimination of marginalisation and social exclusion factors, the prevention of crime, in particular predatory

of such data. This Directive was the main EU legal instrument on data protection until the GDPR came into force. Indeed, it was adopted with the specific aim of harmonising data protection rules to ensure a 'free flow' of data and promote a high level of protection of citizens' fundamental rights.

²³ [Here](#) the DPA set out the fulfilments, guarantees and safeguards already required by the law on the protection of personal data, while awaiting specific legislation regulating the use of video-surveillance systems.

²⁴ They are all available [here](#) and [here](#).

²⁵ Converted with amendments into [Law no. 38/2009](#).

²⁶ Converted with amendments into [Law no. 48/2017](#).



crime, the promotion of a culture of respect for legality and the affirmation of higher levels of social cohesion and civil coexistence”.

The most famous case of use of FRTs by a Municipality was the 2019 pilot project of the Municipality of Como. The Municipality introduced FR functions in the already installed cameras in the area of Viale Tokamachi to upgrade and expand the video surveillance systems²⁷. The Data Protection Impact Assessment specified the purposes of detecting suspects and missing persons, as well as the automatic detection of suspicious and potentially dangerous situations. These purposes fall under the regulation of Legislative Decree no. 51/2018, which transposed the LED. Yet, Legislative Decree 51/2018 does not contain *specific* provisions regarding the collection of biometric data and their storage. On this basis, on 26 February 2020, the DPA interrupted the use of FRTs in Como²⁸.

The interventions of the DPA and the moratorium, now extended until 31 December 2025, have been decisive in banning the use of FRTs in public places and places open to the public. However, the attractiveness of such tools for some Municipalities (see the cases of Turin, Udine, and Lecce²⁹) as well as for the Ministry of the Interior, drove us to try to unveil the *real* intentions of Municipalities and to investigate whether they would be willing to introduce such tools in the future.

In addition, we also examined whether some Municipalities took advantage of the exceptions under Article 9 (12) of Law no. 205/2021, as they could also be considered “competent authorities” for the prevention and suppression of crimes, in line with Article 3 (7) (b) of the LED. This provision encompasses the “body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

To this end, we divided the research on Municipalities into 4 sections, in correspondence to the parts of the questionnaire:

²⁷ The planning of this project was included in the *Documento Unico di Programmazione* (the main tool for the strategic and operational guidance of an Italian Municipality) for the three-year period 2020/2022 of the Municipality of Como on pages 104 and 215. Read it [here](#).

²⁸ The analysis of the [DPA provision](#) of 26 February 2020 can be consulted at 2.4.1. of the [Research Report 1](#).

²⁹ See 2.4.2 and 2.5.1 of the [Research Report 1](#).



- 1) From 2018 to the moratorium of December 2021;
- 2) From 2022 to December 2023;
- 3) For the future (i.e., after the expiration of the sunset clause regarding the moratorium);
- 4) Funds and partnerships.

Since the data collection took place between 1st March and 31st May 2023, section no. 3) considered only the moratorium as regulated by Law no. 205/2021, hence without considering its extension until 2025. However, we do consider the answers as equally valid: firstly, the moratorium cannot be considered a permanent solution within the Italian legal framework; in addition, the main objective of the inquiry was to explore a possible interest in the introduction of FRTs once the ban had been lifted and it can be assumed that the interest would still be valid after the extension.

Few clarifications should be made regarding the specific recipients of the questionnaires within the Municipalities: 1) we contacted the Data Protection Officers, as we assumed they would necessarily be consulted and involved should a Municipality wish to install FRTs; 2) we also approached Public Relation Offices, so that the officials could either answer the questionnaire directly or address it to the competent internal offices. In this sense, we prioritised obtaining a response regardless of the qualification of the recipient. This is also the reason why recipient data was not processed.

All questions were optional, with the exception of the query regarding consent or refusal to process personal data.

Based on the sample identified, we contacted 195 municipalities and obtained 57 replies; out of 195, only 51 recipients accepted the privacy policy and were therefore able to carry out the questionnaire and provide the answers that we illustrate in the following paragraphs.



Map of respondents





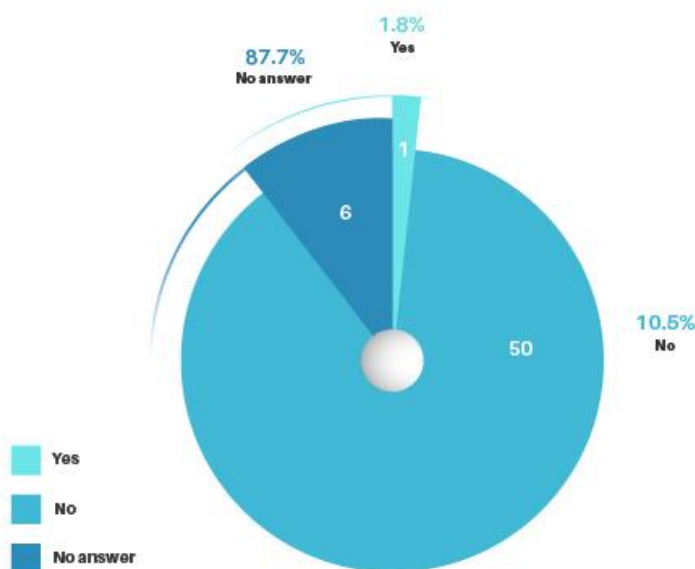
4.1 Before the moratorium

The first section of the questionnaire concerned the period before the moratorium, *i.e.*, before December 2021.

Although the use of FRTs in Italy is relatively recent (since the Ministry of the Interior purchased the SARI software in 2017), the Como case prompted an examination of this timeframe as well. An investigation by *Wired* claimed that these tools had been used unlawfully for several months before the DPA's decision in February 2020 (which led to the dismissal of integrated camera systems with FR functions).³⁰ The aim was to verify whether there were any other unauthorised uses of such systems in other municipalities.

Following the acceptance of the privacy policy of the concerned Municipality, the first question of in this part of the questionnaire was:

1) Did the Municipality use facial recognition technologies before 2022?



Did the Municipality use facial recognition technologies before 2022?

As can be seen in the graph, 6 Municipalities did not accept the privacy policy (10.5%). Of the other 51 Municipalities, 50 (87.7%) stated that they had not used these technologies in the period prior to the moratorium, while only one Municipality (Vibo Valentia) answered positively. The information gathered was, however, limited as the questionnaire's respondents only answered question 1 without providing further explanations in the subsequent sections.

By conducting further research, it became clear that the installation of video surveillance systems has been a central issue for

³⁰ L. Carrer, "Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale", *Wired*, 9 June 2020. Available [here](#).



the administration of Vibo Valentia between 2020-2021. In 2021, the Vibo Valentia Municipal Executive (*Giunta Comunale*) approved an executive project to seek funding from the Ministry of the Interior for the implementation of video surveillance in the city³¹. This initiative was prompted by a surge in crime rates in the city's area. Further evidence of this interest can be found in the map of Municipalities that received funding for video surveillance systems under the Ministry of the Interior's 2020 call for tenders, compiled by *Wired* and based on data published by the Ministry of the Interior³². For instance, the map refers to the Municipality of Vazzano, in the Province of Vibo Valentia, which received almost € 157.000 for the installation of video surveillance infrastructure.

The above data, however, refers only to *video* surveillance and to the Province, with no reference to FR tools or systems and to the Municipality. Consequently, doubts remain as to the accuracy of the answer provided to the questionnaire, which did not allow to figure out if (and if so, when) FRTs have been used in the Municipality of Vibo Valentia before 2022.

Then, the questionnaire continued. In case of an affirmative answer to the question n. 1, the questionnaire allowed the recipients to clarify:

- 2) Through which (formal) act the Municipality had authorised the use of these technologies, the purposes of their use and whether a policy on the processing of personal data had been put in place.**

No answers were provided.

In case of a negative answer to the question n. 1, instead, the questionnaire asked:

³¹ The minute of the deliberation of the Municipal Executive can be found [here](#).

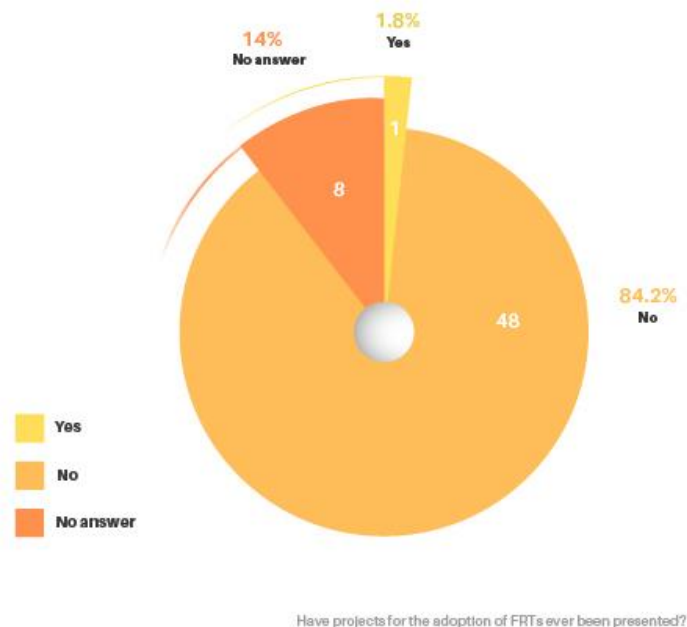
³² Laura Carrer, "Come si finanzia in Italia la videosorveglianza nei Comuni", *Wired*, 26 March 2021. Available [here](#).



3) Have projects for the adoption of FRTs ever been presented?

As shown in the chart, besides those that did not accept the privacy police, two additional Municipalities (Vibo Valentia and Napoli) did not reply (8 in total, 14%). 48 Municipalities (84.2%) claimed that they had not submitted these kinds of projects.

One Municipality (Jesolo), though, **declared the submission of a project**. It is interesting and worth noting that we received two different answers to question n. 3 from different recipients in Jesolo, a local police officer and a PA employee. Of the two, only the local police officer answered “yes” - but without specifying the kind of project submitted.



The result is particularly interesting as it allows to assume that FR systems were not considered by the Municipality before 2022, but **attracted more attention from the local police**, who tried to introduce them for purposes currently unknown. This detail could also open the way for a new investigation directly concerning the local police, in order to understand whether they are interested in using FRTs, perhaps through forms of coordination with the State Police (*Polizia di Stato*).

To conclude, it can be noted that the measure adopted by the DPA against the Municipality of Como in February 2020 had a dissuasive effect, discouraging other Municipalities from adopting FRTs. Before 2022, with the exception of the case of Como, no concrete applications of FRTs were recorded, as demonstrated in our data collection.



4.2 During the moratorium

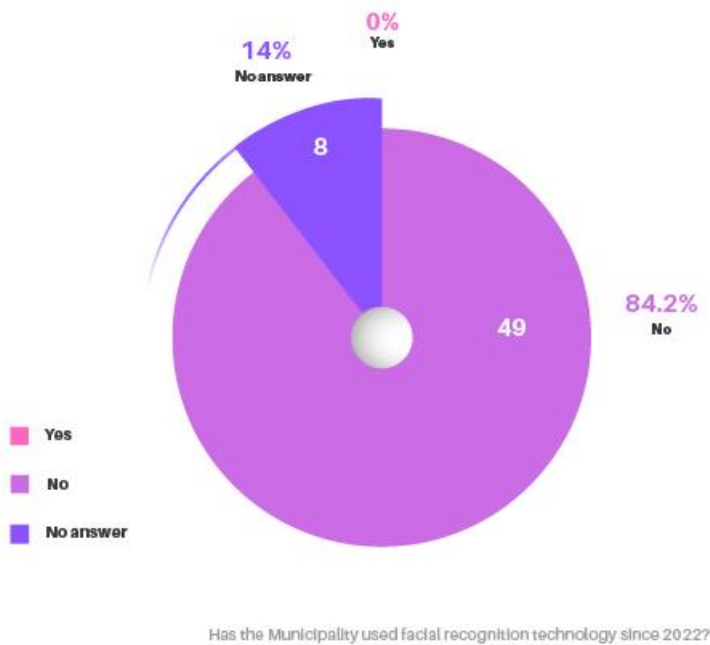
The second part of the questionnaire was dedicated to the period of validity of the first moratorium, namely between January 2022 and December 2023.

The results obtained in the below section are also valid for the two-year period 2023-2025. Indeed, the aim of the research was also to understand whether the Municipalities had interpreted Art. 3 (7) (b) LED extensively, considering themselves as competent authorities and taking advantage of the exceptions of the moratorium to install FRTs for crime prevention and law enforcement purposes; and whether they had started to submit projects to use FRTs once the moratorium would have expired, while waiting for the adoption of the AI Act.

We have repeated the question pattern of the first section, changing the time reference.



4) Has the Municipality used facial recognition technology since 2022?



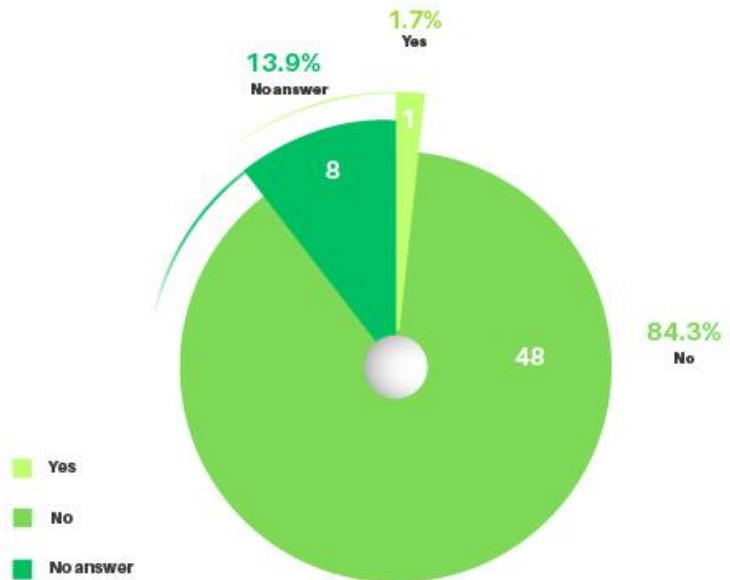
As can be seen from the graph, 8 Municipalities did not respond at all (14%): the six that have not accepted the privacy policy and Vibo Valentia and Napoli. The remaining 49 Municipalities (86%) responded negatively. **No Municipality therefore used FRTs during the moratorium period, demonstrating the importance of the ban placed by the Italian legislator, pending a legal framework at European level that would have standardised the regulations on the matter in the EU Member States.**

In case of a negative answer to this question, the questionnaire continued:



5) Have projects for the adoption of such technologies ever been submitted?

The diagram shows how the same 8 Municipalities already mentioned did not answer the question (13.9%), 48 Municipality (84.3%) provided negative answers, while one Municipality (Lecce) clarified it had presented a project for their adoption. The response came from the local police headquarters, further confirming their interest in these technologies and the future possibility of their involvement in the use of FRTs.



Have projects for the adoption of such technologies ever been submitted?

The municipality of Lecce also indicated the context of the project submitted: it was part of the PON Security 2020 - technical and economic feasibility project for the implementation of an intelligent video surveillance system in the municipality of Lecce. To be more specific, the reference is to the National Operational Programme (PON) Legality 2014-2020. It is a seven-year investment plan managed by the Ministry of the Interior and destined for less developed regions. Its priorities include fighting crime, strengthening legality conditions, and improving security conditions in productive areas and areas of cultural interest³³.

After the Municipality of Lecce's intention to purchase a system involving FRTs was made public, the DPA intervened by opening an inquiry against the Municipality. The DPA requested a description of the systems adopted, the purposes, the legal bases of the processing operations, a list of the data also consulted by the devices, and an impact assessment on the data processing. The DPA stressed, in any case, the impossibility of installing and using FR systems based on biometric data during the period of the moratorium or until a specific law on the matter comes into force³⁴. Conclusively, the DPA's intervention stopped the employment of FRTs in the Municipality of Lecce.

³³ For more information on the Programme consult this [link](#).

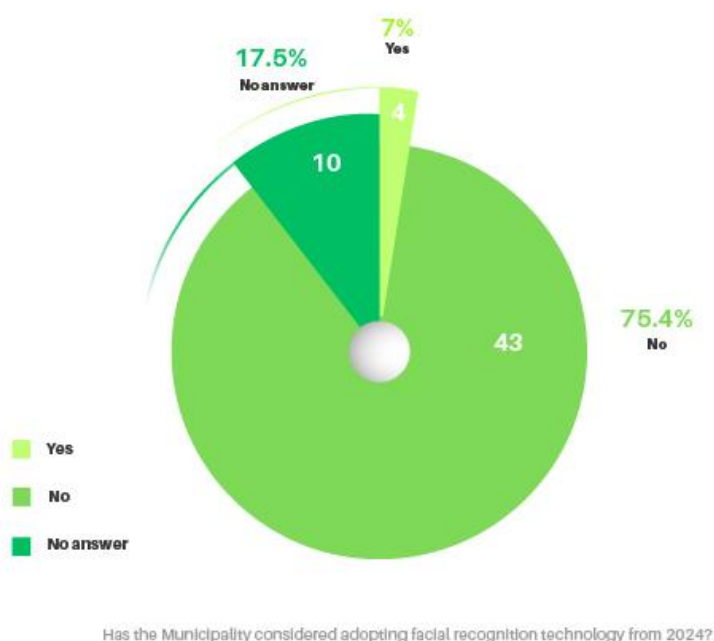
³⁴ Read the DPA notice of 14 November 2022 [here](#).



4.3 After the moratorium

The last section of the questionnaire explored possible *future* interests of Municipalities in purchasing and using FRTs. The question asked was the following:

6) Has the Municipality considered adopting facial recognition technology from 2024?



It is worth pointing out, once again, that the questionnaire was carried out *before* the extension of the moratorium. However, as previously mentioned, the results obtained maintain relevance. Indeed, they map which Municipalities intended to purchase, and use, FRTs in the near future.

As can be seen in the graph, 10 Municipalities did not provide a response (17,5%). This list includes, in addition to the six Municipalities that did not accept the privacy policy, the Municipalities of Vibo Valentia, Napoli, Cagliari, and Cremona. The Municipalities that stated that they had not considered this possibility are 43 (75.4%), **while 4 (Sassari, Firenze, Jesolo, Lecce - 7%) admitted that they had considered introducing FRTs within the Municipality's boundaries**, specifying the purposes that would justify their use.

The Municipality of Sassari explicitly stated that the aim was to implement a video surveillance system in the city. The Municipality of Firenze and the Municipality of Jesolo mentioned security purposes. The reply from the Municipality of **Lecce** was very comprehensive, as the entire programme was detailed: the intention was to strengthen actions to prevent and combat forms of illegality in the municipal area, especially with reference to the area adjacent to the railway and some areas of the historic centre currently monitored by existing video surveillance systems. Through a collaboration between the police forces and the local police, the Municipality would like to **make use of the FRTs and other resources to protect areas of strategic importance from a tourist, artistic and**



architectural point of view, combating loitering, begging, fights, drug dealing, robberies, and property crimes.

In general, it is clear that security is a central issue for municipal administrations, and it is certainly of primary importance to study suitable solutions to fight crime. However, a balance must be struck between security and fundamental rights to avoid making choices that lead outside the perimeter of legality. To date, the use of FRTs must be excluded until the adoption of the EU Regulation on AI, which should take place before the expiry of the moratorium set for 31 December 2025. In light of the forthcoming European regulation, investments should be directed towards areas such as urban redevelopment, social inclusion, and cultural revitalization (as defined under Article 4 of Decree-Law 14/2017), hence contributing to the achievement of good security standards. These areas of focus should address the potential risks associated with these technologies to fundamental rights and freedoms, and aim to eliminate marginalisation and social exclusion.

4.4 Funds and partnerships

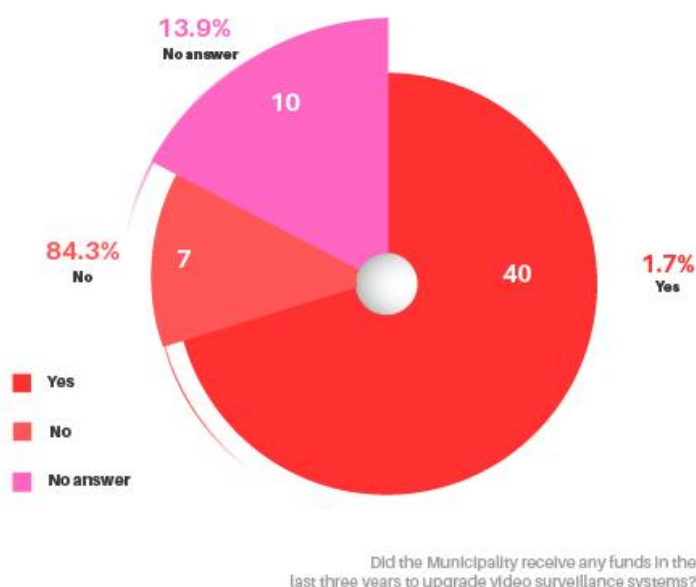
In addition to investigating the situation strictly related to FRTs within Municipalities over a fairly broad time span, we investigated two further parallel profiles:

- i) funding for the implementation of video surveillance system; and
- ii) proposals received by the Municipality from private parties.

Regarding funding for the implementation of video surveillance systems, Municipalities have been asked the following question:



7) Did the Municipality receive any funds in the last three years to upgrade video surveillance systems?



As facial recognition software complements CCTV cameras, feedback beyond the 2022 ranking³⁵ was sought particularly in relation to county towns (which have more money than smaller and less populous municipalities) to cross-reference the data with the answers already collected in the other sections of the questionnaire. Indeed, the installation of FRTs could have taken place or may take place in the future mainly due to this flow of funding for the implementation of the video surveillance cameras.

Graph illustrates that among the 10 Municipalities that left the section on the post-moratorium period incomplete, none of them responded to this question (17.5%). Among the 40 Municipalities that confirmed that they had received funds for video surveillance systems in the last three years (70.2%), the Municipalities of Sassari, Jesolo, and Lecce also explained (in their reply to question n. 6) their **willingness to consider adopting FRTs in the future**. We can assume, therefore, that they will allocate these funds for the possible installation of FR systems.

The 7 Municipalities that affirmed that they had not received funds for the implementation of video surveillance systems recently include Firenze, Enna, Isernia, Langhirano, Brindisi, Albisola Superiore and Catania (12.3%).

The presence of the Municipality of Firenze is worth highlighting, as it had expressed its intention to install FRTs in the near future in the post-moratorium section (q. 6). By this point, we asked ourselves: what could be the factors behind their failure to secure funding for basic video surveillance? It is argued that these factors can essentially be categorised as follows:

³⁵ Read paragraph 2 where it refers to the sampling strategy and footnote 14.



- they did not submit a project application;
- their project did not meet the eligibility requirements;
- their project received a negative assessment, based on factors such as the crime index of the province and municipality, and the incidence of crime in the urban area where the system would be installed.

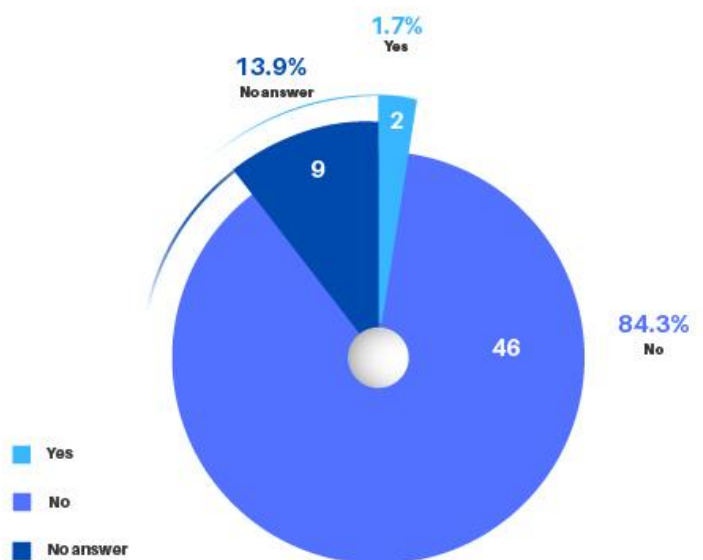
The second profile investigated in this section was:

8) Did the Municipality receive any proposal from private parties (e.g. companies) to explore using FRTs?

We assumed that Municipalities could be solicited by external parties, hence we wanted to find out which ones were most interested in creating partnerships with Municipalities.

As shown in graph, 9 Municipalities did not provide an answer (15.8%). In contrast to the last questions presented –answered negatively, along with 45 other municipalities (46%). On the other hand, two Municipalities, Langhirano and Prato, reported having received proposals of collaboration from private individuals (3.5%).

The Municipality of Langhirano mentioned that they had been contacted to activate facial recognition functions for the SPID service, *i.e.* the Public Digital Identity System that allows citizens and businesses to access online services of PAs and private individuals with a single Digital Identity. This proposal does not raise any particular concerns because the inclusion of the face recognition function would



Did the Municipality receive any proposal from private parties (e.g. companies) to explore using FRTs?



only be used for authentication purposes, replacing the alphanumeric login and password to access a service³⁶.

The reply of the Municipality of **Prato**, on the other hand, is alarming, **as the partnership project envisaged the use of FRTs for the purpose of identifying subjects for reasons of public safety**. In this case, there are numerous critical issues that may arise: the private subject, e.g. a company, could manage the service by having direct access to the biometric data of the persons filmed, with unclear consequences on the preservation and use of the images collected. Above all, it would favour a particularly invasive monitoring of those who circulate in the areas affected by the technology, thus impacting the fundamental rights and freedoms mentioned in the first paragraph and leading to a 'chilling effect' on the free use of public spaces. The company that submitted the project proposal to the Municipality was not named in the answer of the questionnaire, remaining therefore unknown. Nevertheless, the Municipality of Prato does not seem to have accepted the proposal, but the issue may be revisited in the future.

5. Conclusions

The European Court of Human Rights ("the Court") on 4 July 2023 condemned Russia for violating the rights to respect for private life and to freedom of expression (Articles 8 and 10 of the ECHR, respectively). In the *Glukhin v. Russia* judgement³⁷ the Court found that facial recognition was a particularly intrusive tool for identifying a person in order to fine them for the administrative offence of "failing to give prior notice of a solitary and peaceful demonstration", and that a further level of justification was required for the use of this tool in a democratic society. In this case, the lack of a precise and detailed legal framework meant that the police authorities had a wide margin of discretion in deciding whether to use FRTs, without any regard for the guarantees inherent in the rule of law.

This is precisely why we supported the EU Parliament's intervention on the AI Act in a restrictive sense, specifically the naming/including of "post" remote uses of biometric

³⁶ Article 29 Data Protection Working Party, [Opinion 2/2012](#) on facial recognition in online and mobile services, WP 192, 22 march 2012 and [Opinion 3/2012](#) on developments in biometric technologies, WP 193, 27 april 2012.

³⁷ Read the judgement [here](#).



technologies in the list of banned AI systems at EU level (with the only exception of its use for the prosecution of serious crimes, and only after judicial authorisation), in addition to real time biometric surveillance. However, as mentioned above, the outcome might differ from the position adopted by the EP, as negotiations are currently taking place within the Council.

Although the AI Act as such will have direct application in the domestic legal framework of each EU Member State, the adoption of a legislation at national level will be nonetheless necessary to define clear guidelines for the areas in which FRTs will certainly be used, such as law enforcement activities by police forces and judicial authorities.

As a consequence, this second report departed from the initial assumptions and expanded upon the insights gleaned from the first report. Its primary objective was to explore potential avenues for utilising our first [Research Report](#), which contains a toolkit directed at all those interested in strategic litigation in this field. Through a practical approach, we therefore attempted to investigate the possible applications of FRTs by different stakeholders, hoping to break the silence surrounding the topic and to understand new directions for possible future investigations.

However, we were not able to achieve what we had originally planned. In particular, one of the main objectives of this practical approach was to open a channel of communication with the police headquarters and public prosecutors' offices that could have inaugurated a flow of information inspired by transparency. Since the DPA had expressed a favourable opinion towards the use of the SARI-Enterprise system on 26 July 2018, our intention was to shed light on the profiles relating to its possible use. The answers could have provided a basis for critically analysing the strengths and weaknesses of the system, with a particular focus on the impact on fundamental rights and freedoms. Furthermore, we wanted to investigate the frequency of use of these technologies and whether the types of crimes for which they could be used had been identified - despite the absence of a specific legislation.

Starting from this data, we aimed at investigating further aspects, including the error rates recorded over a range of uses of face recognition software; the existence of regular sessions of third party testing and audits to drastically reduce cases of false positives and false negatives (with the aim of eliminating them) and to ensure statistically correct and fair results, avoiding discrimination based on ethnicity or gender; whether the practice of requesting the authorisation of a judge had developed at police headquarters in the absence of a specific discipline; a reflection on the introduction of independent audits and other mechanisms for the accountability of those who use FRTs in order to ensure their ethical use, among others.



As could be seen, however, we did not have the opportunity to delve into the subject because the Police Headquarters did not make themselves available to answer the questionnaire, either due to an autonomous choice or to the lack of authorisation that should have been granted by the State Police External Relations Department. As far as the Public Prosecutor's Offices are concerned, only four replies were obtained, all containing the declaration of non-use of FRTs.

In the absence of information, we intensified our open source research. However, the lack of publicity surrounding the use of FRTs made it difficult to access up-to-date and accurate information, or any information at all. Thanks to the first Report, we learned of two uses of SARI-Enterprise: one took place in Milan in 2020. A public prosecutor used the tool to identify the faces of five people involved in a brawl and to request the application of a pre-trial detention measure on one person. The other case concerns the use by the police in January 2023 to identify a suspect guilty of the attempted murder of a young tourist at Roma Termini station³⁸.

We recently learned of another case of SARI-Enterprise being used through an article published in *Ansa*, an Italian news agency. On 9 August 2023, SARI was used to identify the attacker of a bus conductor in Pescara, who was later charged with the offences of aggravated injuries, violence and threats to a public official as well as interruption of a public service and hit-and-run after subsequent findings confirmed the identity³⁹. Despite recognising the importance of the necessary and unavoidable human feedback after the alert generated by the system and the reliability of the outcomes in these cases, doubts remain as to whether SARI was not used more frequently and only produced reliable results.

More interesting results emerged, on the other hand, at the outcome of the research that targeted Municipalities. Unfortunately, we received no response from the Municipality of Como (the only one to have actually used FRTs by integrating them with video surveillance cameras in a critical area of the city). Similarly, no response was recorded from the Municipality of Udine, which was very interested in the introduction of these technologies for public safety purposes, as was also recently stated by Mayor Pietro Fontanini at the "Sicurezza Città di Udine" 2023 event⁴⁰.

As the graphs and the processing of the collected data shown, the most relevant results were found with reference to the intentions of *future* uses of FRTs. The intervention of the

³⁸ At pages 34-35 of the [First Report](#).

³⁹ Redazione Ansa, "Aggredisce controllore a Pescara, individuato grazie all'IA", Ansa, 13 agosto 2023. Read the news [here](#).

⁴⁰ [Here](#) is the recording of the morning session of the event on 3 March 2023.



DPA against Como in 2020 and the “second” moratorium from 2024-2025 have effectively prevented any initiatives by Municipalities to use these technologies. However, some Municipalities have expressed their intention to use them to fight crime and ensure citizen safety. In fact, 7% of those who filled out the questionnaire were in favour of opening up to face recognition systems

Nevertheless, the public security purposes put forward to justify the willingness to adopt these tools by some Municipalities must be balanced with the high crime rates increased in recent years: this will allow to understand whether the policies in the pipeline concerning the deployment of video-surveillance systems, and possibly FRTs, will be based on real security or perceived security problems.

Since the future projection will have to be postponed until the moratorium expires, we compared the most recent general crime index rankings, prepared by the newspaper *Il Sole 24 ore* on the basis of data from the Department of Public Security of the Ministry of the Interior⁴¹, which describes in detail the complaints related to the total number of crimes committed on the territory of the 106 Italian Provinces⁴². It was not possible to compare the Municipalities directly due to a lack of data, but we decided to use the parameter of the Provinces in order to have a result that could be considered as reliable as possible.

The Province of Firenze is one of the most dangerous in Italy, as 42.957 complaints were recorded in 2021 and 47.028 in 2022; the Province of Sassari is positioned about halfway down the ranking as in 2021 there were 13.455 complaints, while in 2022 there were 14.259; the Province of Lecce, on the other hand, is located further down, around 70th position, recording 20.278 complaints in 2021 and 21.204 in 2022⁴³. The numbers of complaints seem to be on the rise, but these Provinces still lose places in the ranking, showing the trend of decreasing offences in Italy.

At this point, it is worth considering the usefulness of this continued investment in CCTV and the improvements that CCTV could bring. It is not disputed that administrations should pursue the security needs of citizens living in the area, but a broader reflection on the

⁴¹ Check the rankings [here](#). The data of the Crime Index photograph every year the crimes that emerged during the previous 12 months following the reports of the Police Forces (Polizia di Stato, Carabinieri, Guardia di Finanza, Corpo Forestale dello Stato, Polizia Penitenziaria, DIA, Polizia Municipale, Polizia Provinciale, Guardia Costiera).

⁴² The final ranking takes into account the following crimes: intentional homicide, attempted homicide, sexual assault, theft, car theft, shop theft, burglary, robbery, extortion, usury, criminal conspiracy, mafia conspiracy, money laundering, fraud and computer fraud, arson, drug trafficking.

⁴³ Jesolo remains out of this comparison as it is not a Province, but there have been numerous episodes of violence reported in recent years.



allocation of public expenditure should be developed. In the absence of clear improvements, it would be necessary to reconsider a different management of funds, which should also be allocated, as a priority, to strengthening social services. The considerable resources devoted to the implementation of video surveillance systems have not produced the desired results, as CCTV has not even achieved excellent results in terms of deterrence. There are therefore other ways of tackling the security problems, which are highly transversal and affect northern, southern and central Italy equally.

Although this report has been a first step in problematising the use of FRTs, we hope that it has laid the foundations for future research. The hope is that future inquiries will be based on the assumption that indulging in securitarian policies to the detriment of fundamental rights and freedoms is not the only solution available. Above all, it is always necessary to carry out a cost-benefit assessment, without blindly relying on control technologies such as FRTs, which risk compromising the foundations of the rule of law, with no possibility of turning back later.