Building a litigation strategy
to challenge the use of

FACIAL RECOGNITION TECHNOLOGIES

by law enforcement and judicial
authorities in Italy

Executive summary

StraLi - For Strategic Litigation

www.strali.org
info@strali.org

Executive summary

About StraLi

StraLi is an NGO founded in Italy in 2018 by lawyers and legal practitioners to respond to inequities in the law and violations of human rights. It obtained a pre-litigation research support grant from the Digital Freedom Fund 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?

Context and Relevance of the Research

In October 2021, the Italian government enacted Decree Law 139/2021, suspending the installation and use of FRTs in public spaces. Yet, this "moratorium" does not apply to judicial authorities, public prosecutors, and police agencies using FRTs for the prevention, investigation, detection, and prosecution of criminal offences. This research project focuses on three sub-questions: how Italian law enforcement agencies (“LEAs”) and judicial authorities use FRTs, whether the use of FRTs in the criminal trial is compatible with the national/supranational legal framework, and what remedies are available to challenge this practice and/or the moratorium. The research focuses on pertinent decisions made by Italian and other national/supranational courts, the European Court of Human Rights, and the Court of Justice of the European Union.

The goal of the research report is to determine before which authority(ies) we should bring our proposed strategic litigation. It is also meant to serve as a toolkit for other NGOs in the planning of their litigation strategies.

Structure of Research Report

The Research Report is structured as follows:

- Chapter 1 - Introduction
- Chapter 2 - The Italian Case
- Chapter 3 - European Court of Human Rights case law on Articles 6, 8 and 10 of the ECHR in combination with Article 14 ECHR
- Chapter 4 - European Court of Justice case law on Articles 8, 11, 21, 4, 1 and 47 of the Charter of Fundamental Rights of the European Union and Regulation 679/2016 (GDPR)
- Chapter 5 - Decisions, recommendations and reports of National Data Protection Authorities and other European/international privacy watchdogs or institutions

Chapter 2 - The Italian Case

In January 2017, the Ministry of the Interior purchased the Automated Image Recognition System (“SARI”) software to support investigative activities and forensic police surveillance.
SARI is based on two modules: SARI-Enterprise and SARI-Real-Time. SARI-Enterprise can be used to compare an image frame with the A.F.I.S. database (Automated fingerprint identification system), integrated by the S.S.A. (Sottosistema anagrafico, a database containing mug shots of subjects). SARI Real Time uses a series of cameras installed in a defined geographical area to analyse in real time the faces of people filmed in that area. This is done by comparing them with a predefined database for the specific service (called the "watch list"), the size of which is limited to a maximum of 10,000 faces.

The use of SARI-Enterprise was approved by the Italian DPA in July 2018. The use of SARI-Real Time, instead, was subject to a negative decision of the Italian DPA in March 2021. There is no independent oversight on either the composition of the AFIS-SSA database nor on the use of SARI-Enterprise applied to such database.

In December 2021, Italy approved a moratorium on FR systems in public places or places open to the public until the end of December 2023. Nevertheless, the law also establishes an important exception to the ban: the processing of biometric data carried out by “competent authorities” for the purposes of preventing and repressing crimes or executing criminal sanction according to Legislative Decree 51/2018 (which implemented the LED Directive in the Italian legal system).

As of today, there is no Italian case law specifically on SARI-Enterprise. On the other hand, there have been multiple newspaper articles reporting that it was used to successfully complete an investigation and one judgment by the Corte di Cassazione referring to its results to support the request of a pre-trial retention measure by a public prosecutor.

Using FRT as evidence in a criminal trial must be confronted with due process as enshrined in the Italian Constitution and in other supranational legal systems, specifically with the principle of adversarial proceedings. This means that every party in a trial has the right to support its case through evidence and to rebut the other parties' evidence. The Italian Code of Criminal Procedure distinguishes between "evidence" and "evidence-gathering tools" and regulates numerous types of evidence, referred to as "typical". In 1988, the Italian legislator introduced the category of "atypical evidence", which is now governed by Article 189 of the Code. Evidence not regulated by law may be admitted if it is suitable to ensure the establishment of facts and does not prejudice the person's moral freedom of the person.

FRT is not expressly regulated in the Italian Criminal Code of Procedure. Its functioning is obscure to the parties involved, and the lack of transparency is enhanced by AI’s intrinsic characteristics.

Hence, the Research Report discusses two main issues in this regard:

1. Whether the output produced by a FR system, such as SARI-Enterprise, could qualify as a new form of scientific evidence, and therefore could “enter” the criminal trial via art. 189 of the Italian Code of Criminal Procedure, which regulates the category of “atypical evidence”;
2. Whether the use of SARI could be reconducted to article 361 of the Code of Criminal Procedure, which regulates the identifications of suspects during investigations.

This chapter is concluded with an overview on purchases, and uses, of FRTs by local administrations for purposes of ensuring “public safety”.

Chapter 3 - **European Court of Human Rights case law on Articles 6, 8 and 10 of the ECHR in combination with Article 14 ECHR**

The chapter examines the use of FRT in criminal proceedings and its implications for various rights protected under the European Convention on Human Rights (ECHR). It focuses on Article 6, which guarantees the right to a fair trial; Article 8, which protects the right to privacy; and Articles 10 and 11, which safeguard freedom of expression and freedom of assembly and association.

Regarding Article 6, while there are no specific decisions on FRTs by the European Court of Human Rights (ECtHR), the principles established in its case law can still find application. The lack of transparency and understanding of FRTs can hinder the defense's ability to challenge its admissibility, potentially affecting the fairness of the trial. The use of FRTs in criminal proceedings raises concerns about the equality of arms, the admissibility of evidence, and the presumption of innocence.

In relation to Article 8, the ECtHR has addressed cases involving mass surveillance, artificial intelligence, and FRTs. Compliance with the Convention has been evaluated in cases such as Centrum för Rättvisa v. Sweden and Big Brother Watch and others v. the UK. The ECtHR plays a crucial role in assessing the compatibility of FRTs and mass surveillance with fundamental rights, emphasizing the need for appropriate safeguards and proportionality assessments to protect individuals' rights.

In relation to Articles 10 and 11, the use of FRTs can have a chilling effect on society and hinder the exercise of the rights of freedom of expression and freedom of assembly. While there is no direct case-law addressing the combination of Articles 10 or 11 with Article 14 (which prohibits discrimination in the enjoyment of Convention rights), the adverse effects of FRTs on the exercise of these rights are evident, particularly with live FR systems.

While requiring the respect of the principles of necessity and proportionality according to Convention 108+ (as well as to ECHR), the CoE’s Guidelines on Facial Recognition of January 2021 allow domestic law to provide for different necessity and proportionality tests based on the purpose for which the FRT has been used by LEAs, namely verification or identification.

When it comes to the employment of live FRT (like SARI- Real Time in the Italian context), national law has to ensure that LEAs can prove that several factors, such as the time and place of deployment of such technologies, comply with the strict necessity and proportionality test.

The main issue tackled in this part of the Report is understanding how judicial systems are (or will be) able to deal with technological developments – including FRT – without (arbitrary) refraining from safeguarding the due process guarantees and related principles and thus, by framing the use of such tools to ensure fundamental rights within criminal proceedings.

In fact, relying on the above-mentioned ECHR and Convention 108+ principles and provisions, and linking the employment of AI tools (including FRT) within criminal justice systems, in 2018 the European Commission for the Efficiency of Justice (CEPEJ) of the CoE adopted the "European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" ("the European Ethical Charter").

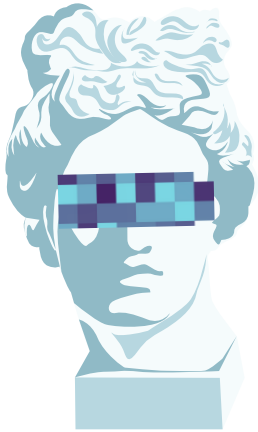
The European Ethical Charter emphasizes three key principles related to the analysis of judicial data through computational systems:

- the principle of non-discrimination;

- the principle of quality and security of data;

- the principle of transparency, impartiality and fairness.

In the context of evaluating evidence in criminal proceedings within the Italian system, where judges are required to explicitly assess the reliability of each piece of evidence, mere "algorithmic transparency" is insufficient to provide a clear understanding of the process behind generating digital evidence. This lack of clarity may undermine the trustworthiness of the decision in the eyes of recipients and the public.



Chapter 4 - CJEU case law on Articles 8, 11, 21, 41 and 47 of the Charter of Fundamental Rights of the European Union and Regulation 679/2016 (GDPR)

The Chapter is focused on the impact of FRTs and AI on fundamental rights within the European Union. The discussion revolves around the interpretation of privacy, limitations on rights, discrimination, good administration, and access to effective judicial remedies.

The discussion highlights the interpretation and rulings of the Court of Justice of the European Union (CJEU) on these issues.

● Privacy and Data Protection:

The CJEU recognizes privacy as a central aspect of data protection law. In a recent decision of 2023 (Ministerstvo na vatreshnite raboti), the CJEU analyzed the requirement of "provided for by law" in the context of a tax fraud criminal case, where the defendant objected to the collection of her biometric and genetic data. The CJEU has consistently emphasized that the invoked public interest is not enough to limit the rights enshrined in the Charter, specifically Articles 7 and 8. Although there are currently no CJEU rulings on the use of FRTs concerning the violation of Articles 7 and 8 of the Charter, the principles referred to this rights may also apply in this case. Regarding the use of SARI Real-Time, in light of the Court's findings in the various cases examined, the requirements of Articles 8 (2) and 52 (1) for the limitation of fundamental rights cannot be considered fulfilled.

● Freedom of expression and freedom of assembly:

The Charter's freedom of expression and assembly rights align with the European Convention on Human Rights (ECHR). Limitations on these freedoms should adhere to ECHR standards, being prescribed by law and necessary in a democratic society. While there are no previous CJEU decisions on the infringement of these rights by FRTs or AI, the principles still apply.

● Discrimination:

The Charter's right to non-discrimination extends beyond the grounds listed in the ECHR. Biases in the data used for algorithm development contribute to biases in FRTs. Lack of representation in training data leads to difficulties in accurately identifying individuals with darker skin tones or different ethnic origins. Predictive policing software can perpetuate existing systemic flaws and injustices. The lack of transparency in the functioning of algorithms and the databases used exacerbates these concerns.

As pointed out by Hermes, apart from the lack of knowledge of the functioning mechanisms of the algorithms used, there is no precise information available on the number of people included in this database who are then included in the AFIS-SSA database, where the images, fingerprints, and personal data of people under criminal investigation or deemed dangerous or suspicious by public authorities also converge.

This database is then used in conjunction with SARI-Enterprise, whose algorithms are harbingers of bias, particularly with regard to individuals with darker skin tones or non-Caucasian ethnicity.

● Good Administration:

The right to good administration is a well-established principle in EU law, applying to all EU bodies, institutions, and agencies. In criminal proceedings, the right of access to files must be balanced with the principle of non-disclosure. The right to good administration also applies when AI systems, including FRTs, process personal data and support the decision-making processes of public authorities involved in criminal trials.

● Access to Judicial Remedies:

Article 47 of the Charter guarantees the right to an effective remedy before a tribunal, and member states must establish national systems of remedies adhering to European standards. The CJEU's rulings emphasize the compatibility of Articles 47 and 48 of the Charter with national legislation. Regarding the use of FRTs (or AI more generally) within criminal proceedings, and their impact on the right at stake, in Ministerstvo na vatreshnite raboti the CJEU was called upon to assess the compatibility of Articles 47 and 48 (which safeguard the presumption of innocence and right of defence) of the Charter with the Bulgarian legislation.

The CJEU also points out that the limitation to the right to personal data must, firstly, be prescribed by law and secondly, that the essential content of the right to an effective remedy must be respected. In the light of the above-mentioned clarifications, it can be argued that Italian legislation must also be compatible with the right at stake in case of collection of biometric and genetic data. However, it is necessary for the Italian legislation to provide for a specific provision on the coercive collection of biometric and genetic data of persons subject to a criminal investigation, as well as a specific remedy for the verification of the proper processing of personal data in order not to incur the violation of Article 47 of the Charter.

In conclusion, the use of FRTs and AI within the European Union raises significant concerns regarding privacy, limitations on rights, discrimination, good administration, and access to effective judicial remedies. The CJEU's interpretation and rulings highlight the need for robust safeguards to protect fundamental rights in the face of advancing technologies.

Chapter 5 - Decisions, Recommendations

Law enforcement use of FRT poses a number of difficulties due to potential system errors or abuses. NIST research revealed that some FRT algorithms had "undetectable" variations in accuracy across racial groupings, leading to the arrest and detention of an innocent African American man in 2018, among numerous examples investigated. Global policy activity has been intensified due to these concerns, with US technology companies imposing new restrictions and controls on all FRT uses. The use of biometric data and FRT in many situations can interfere with the data subject's fundamental rights, such as Articles 7 and 8 of the EU Charter. FR systems have potential for bias and discrimination due to demographic factors. Data protection law requires that any use of personal information must be lawful, necessary, fair, and proportionate.

FRT should be used by trained professionals, vendors should adhere to standards, ex-ante and ex-post evaluation strategies should be used, European Ethical Charter should be followed, processing of probe images and reference databases should be done in accordance with laws and policies, and most recent findings in machine learning and remote biometrics research should be made available to or facilitated by law enforcement entities. Authorities should conduct impact assessments and consult with marginalised groups to discuss mitigation measures. Clear and effective accountability mechanisms should be established and maintained, and training should be provided for all users. All privacy rules should be followed and data protection principles must be taken into account. Data subjects may not understand when and when FR is used, how and why their data is processed, or how to exercise their rights.

The ICO's review of DPIAs identified a lack of due diligence on the part of controllers. Data quality used to develop and deploy facial recognition has a significant impact on accuracy. LEAs should alert the technology vendor to any pertinent problems and prepare for routine updates or replacements of the FRT. AI systems such as FRT can raise data protection risks, such as statistical accuracy, which can lead to false positives or false negatives. Routine correction and updating of facial photos saved in a watch list is necessary.

Conclusions

Upon the commencement of this research, we hypothesised the possibility of raising a question constitutionality on the compatibility of Article 9 (12) of law 205/2021 with the Italian Constitution. Thus, from a first analysis of the applicable law and of the specificities of the Italian context there seems to be little room for a constitutional claim, since the moratorium “expires” at the end of December. The most probable outcome is a re-expansion of the regulation applicable before the enactment of the moratorium. StraLi has sent municipalities and police headquarters questionnaires to collect data on the matter. The results of the research will be analysed in the next phase.

The use of SARI (or other FR tools) by LEAs could be brought to the DPA for a number of reasons. The DPA is competent on the enforcement of the LED and can be triggered via complaints. It also has a general competence to monitor technological and social developments that affect the protection of personal data. Finally, it could be possible to bring a claim regarding the transparency and composition of the AFIS-SSA database. However, the Italian DPA is not competent to judge on data processing operations undertaken by courts. The only way to challenge the use of SARI by judicial authorities is through the criminal trial and its rules. To do this, it is necessary to search for a "pilot case" in which outputs of SARI have entered a criminal trial. A strategic solution is to obtain a ruling from the Corte di Cassazione on the legitimacy of treating FR-evidence as atypical evidence.

The use of FRT by law enforcement and judicial authorities in the Italian legal framework would likely violate Article 6 of the ECHR, which protects the right to a fair trial. The deployment of SARI as currently normed (and of FRT more generally) within the Italian criminal system would most likely imply a violation of such fundamental right in its declinations of “equality of arms”, “admissibility of evidence” and “presumption of innocence” as “burden of proof”.

The European Convention on Human Rights (ECtHR) has developed the three-part test to determine if a derogation to the right to a private life is lawful. The derogation must pursue one of the legitimate aims listed by the relevant norm, be necessary and proportional, and be in accordance with the law. SARI Real-Time was considered by the Italian DPA as lacking the sufficient legal basis and the Strasbourg Court would assume that this will also be the approach if the Italian legislation remains unchanged. The next step of the research would try to understand whether a submission to the ECtHR can be the most strategic path to challenge the Italian legislation at stake.

The CJEU established proportionality between the use of FRTs and fundamental rights sacrificed, deeming the general or special prevention objective to be preponderant. It also took a residual position with regard to the balance between freedom of expression and data protection, but not directly assessed the impact of FRTs on freedoms of expression and association.

However, the impact of FRTs on the freedoms of expression and association, the right to non-discrimination, and the right to access personal data was not directly assessed by the CJEU.

FRT has a variety of implications for fundamental rights, particularly in law enforcement and criminal justice. It is important to monitor developments in FR by independent supervisory agencies and have sufficient authority, resources, and knowledge to prevent and assist victims. FRT deployment and use must be governed by a comprehensive legislative framework.

The Research was conducted for StraLi by:
Alice Giannini, Federica Genovesi
Mignon van der Westhuizen
Serena Zanirato

With the contribution of:
Laura Carrer, Hermes Center for Transparency and Digital Human Rights

External reviewer:
Lorenzo Sottile, University of Genova

The research is funded by the Digital Freedom Fund as part of their pre-litigation research support.