STRALI
FOR STRATEGIC LITIGATION

Research Report 1

Building a litigation strategy
to challenge the use of

FACIAL RECOGNITION TECHNOLOGIES

by law enforcement and judicial
authorities in Italy

A study of the applicable legal framework at the national, international, and European levels, accompanied by relevant jurisprudence.

StraLi - For Strategic Litigation

www.strali.org
info@strali.org

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.

The information contained in this report is updated until 15/5/2023

Building a litigation strategy to challenge the use of facial recognition technologies by law enforcement and judicial authorities in Italy

Table of contents

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-juridical support given. StraLi successfully obtained a pre-litigation research support grant from Digital Freedom Fund[1] 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 nature of this proposal was determined by particular national circumstances. In October 2021, the Italian Government enacted Decree Law 139/2021,[2] suspending the installation and use of FRTs in public spaces by both private and public actors (Article 9 (9) until the entry into force of legislative regulation of the matter and in any case until no later than December 31, 2023. Yet, the norm provides for two exclusions, namely (A) the suspension does not apply to judicial authorities, public prosecutors and police agencies using FRTs for the prevention, investigation, detection, and prosecution of criminal offences, or the execution of criminal penalties; and (B) in case FRTs are deployed by judicial authorities and public prosecutors for the purposes mentioned before, no preemptive control from the Italian Data Protection Authority ("DPA") is required. The result is that this troubling practice is not subject to any restrictions at all. Furthermore, **the Italian Parliament has not approved, nor even discussed, the adoption of new legislation on the matter.** It is likely then that the moratorium will be lifted without

[1] The purpose of the Digital Freedom Fund is to assist the European digital rights community in advancing and defending human rights in online environments while minimising the detrimental effects of technology on society. DFF provides litigation grants, links partners with professional pro bono assistance, and works to spur legal action. The DFF funds both litigation and pre-litigation research.

[2] Converted into Law 205/2021.

any meaningful change in legislation. The new law settles for a lower standard of protection as a result of the exclusion, falling short of matching the guarantees offered by the dominating position of European and international actors.

This research project develops around three sub-questions. The first is how FRTs are used by Italian law enforcement agencies (LEAs) and judicial authorities to impact the fundamental rights of the individual (e.g., right to privacy, right to a fair trial and an effective remedy, right to non-discrimination), and the guarantees provided by criminal and administrative procedure rules. The second is whether the use of FRTs in this way by the Italian authorities is compatible with the national/supranational legal framework. Lastly, what are the remedies available both at the national and international/European levels to challenge this practice and/or Law 205/2021?

We will be able to determine whether the application of FRTs by Italian law enforcement and judicial authorities is consistent with the fundamental rights framework as established at the national, international, and European levels only by having a clear picture of such framework. This is the purpose of this report and it will allow us to respond to sub-questions n. (1) and n. (2) as described above. We will perform research on pertinent decisions made by Italian and other national/supranational courts, the European Court of Human Rights ("ECtHR"), and the Court of Justice of the European Union ("CJEU") during this phase. Altogether, it is hoped that this research will work as a theoretical basis for building a strong strategy for future litigation. When answering sub-question n. (3), we will evaluate four available paths to challenge the use of FR technologies in the context of criminal justice. The four available paths are:

1. A claim on the compatibility of Article 9 (12) of law 205/2021 with the Italian

Constitution, which under Italian Law has to be raised in an ordinary (criminal) proceeding, in order to obtain a referral to the Italian Constitutional Court;

2. A case in front of the European Court of Human Rights to claim the incompatibility of the referred practice (and the related law) with Articles 6 and 8 European Convention on Human Rights ("ECHR");
3. A claim before the Court of Justice of the European Union to argue the incompatibility of the referred practice (and the related law) with Articles 8 and 47 of the Charter of Fundamental Rights of the European Union, with secondary EU legislation (such as relevant Directive(s) and Regulation(s)) and the overall EU policy on the matter;
4. A complaint to the European Commission claiming the infringement of EU law by the Italian authorities (in the case at stake, the Italian Parliament).

Our goal is to determine before which authority(ies) we should bring our proposed strategic litigation. This research report will not only be of use to us to further our strategic litigation goals but it is also envisioned as a toolkit for other NGOs in the planning of their litigation strategy.

2. The Italian Case

2.1. Due process

Article 111 of the Italian Constitution portrays due process as a condition of the legitimacy of the judicial function. It is connected to the concepts of *discovery* and *equality of arms.*[3] Consequently, it entails the right of the defendant to enjoy the time and facilities necessary to prepare his/her defence.

Art. 111 Italian Constitution	
ITALIAN TEXT	**ENGLISH TEXT**
1. La giurisdizione si attua mediante il **giusto processo** regolato dalla legge.	1. Jurisdiction is implemented through **due process** regulated by law.
2. Ogni processo si svolge nel **contraddittorio tra le parti**, in condizioni di parità, davanti a giudice terzo e imparziale. La legge ne assicura la ragionevole durata.	2. All court trials are conducted with **adversary proceedings** and the parties are entitled to equal conditions before an impartial judge in a third-party position. The law provides for a reasonable duration of trials.

[3] Laura Bartoli, *Parità delle armi e* discovery *digitale: qualche indicazione da Strasburgo,* La legislazione penale, 2022.

3. Nel processo penale, la legge assicura che la persona accusata di un reato sia, nel più breve tempo possibile, informata riservatamente della natura e dei motivi dell'accusa elevata a suo carico; disponga del **tempo e delle condizioni necessari per preparare la sua difesa**; abbia la facoltà, davanti al giudice, di interrogare o di far interrogare le persone che rendono dichiarazioni a suo carico, di ottenere la convocazione e l'interrogatorio di persone a sua difesa nelle stesse condizioni dell'accusa e l'acquisizione di ogni altro mezzo di prova a suo favore; sia assistita da un interprete se non comprende o non parla la lingua impiegata nel processo.	3. In criminal law trials, the law provides that the alleged offender shall be promptly informed confidentially of the nature and reasons for the charges that are brought and shall have **adequate time and conditions to prepare a defence**. The defendant shall have the right to cross-examine or to have cross-examined before a judge the persons making accusations and to summon and examine persons for the defence in the same conditions as the prosecution, as well as the right to produce all other evidence in favour of the defence. The defendant is entitled to the assistance of an interpreter in the case that he or she does not speak or understand the language in which the court proceedings are conducted.
4. Il processo penale è regolato dal **principio del contraddittorio** nella **formazione della prova**. La colpevolezza dell'imputato non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre volontariamente sottratto	4. In criminal law proceedings, the **formation of evidence** is based on the principle of **adversary hearings**. The guilt of the defendant cannot be established on the basis of statements by persons who, out of their own free choice, have always voluntarily

all'interrogatorio da parte dell'imputato o del suo difensore.	avoided undergoing cross-examination by the defendant or the defence counsel.
5. La legge regola i casi in cui la formazione della prova non ha luogo in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva o per effetto di provata condotta illecita.	5. The law regulates the cases in which the formation of evidence does not occur in an adversary proceeding with the consent of the defendant or owing to reasons of ascertained objective impossibility or proven illicit conduct.
6. Tutti i provvedimenti giurisdizionali devono essere motivati.	6. All judicial decisions shall include a statement of reasons.
7. Contro le sentenze e contro i provvedimenti sulla libertà personale, pronunciati dagli organi giurisdizionali ordinari o speciali, è sempre ammesso ricorso in Cassazione per violazione di legge. Si può derogare a tale norma soltanto per le sentenze dei tribunali militari in tempo di guerra.	7. Appeals to the Court of Cassation in cases of violations of the law are always allowed against sentences and against measures affecting personal freedom pronounced by ordinary and special courts. This rule can only be waived in cases of sentences by military tribunals in time of war.
8. Contro le decisioni del Consiglio di Stato e della Corte dei conti il ricorso in Cassazione è ammesso per i soli motivi inerenti alla giurisdizione.	8. Appeals to the Court of Cassation against decisions of the Council of State and the Court of Accounts are permitted only for reasons of jurisdiction.

According to the Italian Constitution, the hard core of *due process* is enshrined in the principle of **adversarial proceedings** (i.e., no one can be subjected to the consequences of a judgement without having had the opportunity to be a party to the process from which it originates or without actual participation in the formation of the judicial decision). If the criminal trial is based on the principle of adversary hearing, it follows that every party in a trial has, on the one hand, the right to support its case through evidence and, on the other, **the right to rebut the other parties' evidence.**

The adversarial nature of proceedings is interpreted as having both an objective and a subjective dimension.[4] From an *objective* point of view, the adversarial nature of the trial is to be found "in the formation of the evidence," i.e., as a method to ascertain the (judicial) truth, as enshrined in para. 4 of art. 111 Const. Only the evidence, which is subject to "rebuttal" by the defendant, i.e., through cross-examination, can be deemed reliable. From a *subjective* point of view, adversary refers to the individual guarantees that are established by the principle in favour of the defendant, e.g., the right of the accused to confront his or her accuser.

The principle of due process is strictly connected to the role of (scientific) evidence in criminal trials. Scientific evidence must respect the rules of criminal procedure before – and after – it enters a criminal trial.

2.2. The Italian Code of Criminal Procedure

The Italian Code of Criminal Procedure distinguishes between "evidence" and "evidence-gathering tools". The first category comprises evidentiary elements

[4] See Corte cost., 25 ottobre 2000, n. 440.

which can be used directly by a judge in his/her decision (e.g., a testimony); the second comprises means of acquiring material items, traces, or statements which could acquire evidentiary significance (e.g., wiretapping).

The Code expressly regulates numerous types of evidence, referred to as “typical”. In 1988, the Italian legislator introduced the category of “atypical evidence”, i.e., evidence that is not expressly regulated in the Code of Criminal Procedure, which is now governed by Article 189 of the Code.

Art. 189 reads as follows:

> When evidence not regulated by law is required, the judge may admit it if it is suitable to ensure the establishment of facts and does not prejudice the moral freedom of the person. The judge shall rule on the admission after hearing the parties on the procedure for taking such evidence.

Consequently, parties have the right to cross-examination when the judge is called upon deciding on the admission of the evidence. This principle was stated by the Corte di Cassazione, Sez. Un. in the *Prisco* Judgement.[5]

It should be specified that this "open" category does not justify more freedoms in the gathering of the evidence than already regulated, for which it is the Code that expressly provides for limits and application. The category of “atypical evidence” is the result of a balancing act between safeguarding the rights of the accused, on the one hand, and making sure that the criminal trial keeps pace with scientific and technological progress, on the other.[6] However, even though art. 189 was inserted

[5] Cass., Sez. Un., 28 marzo 2006, n. 262795.
[6] Amalia M. Buzura, *Nuove forme di atipicità probatoria in materia di videoregistrazioni investigative*, Archivio Penale 2022, n.1, 16.

into the Code more than twenty years ago, and technological progress has made it necessary to deal with this category of evidence, no 'new' evidence is to be found in the case law that does not fall within the typical models.[7]

In January 2017, the Ministry of the Interior purchased Automated Image Recognition System ("SARI") software to support investigative activities and forensic police surveillance. The specificities of such a system will be analysed in the following paragraph.

2.3. Automatic Image Recognition System ("SARI")

SARI operates through two algorithms, one developed by an Italian company, *Parsec 3.26*, and one developed in the U.S. by *Neurotechnology*. It is based on two different "modules": SARI-*Enterprise* and SARI-*Real-Time*. Its core functioning is to search for characteristic points on the image of a face in frontal vision: these can be characterising points, mainly in the area of the eyes, nasal pyramid and chin, i.e., the so-called anatomically precise or "fiduciary points" (which constitute skin projections of bony landmarks, and, as such, tend to be unchangeable over time).[8] According to a performance evaluation conducted on SARI Enterprise in November 2016, mentioned in IrpiMedia's investigation, SARI's accuracy in a database which contains face images of non-white people amounts to 77%. As of today, no further information has been provided regarding the reliability of SARI. Such a lack of transparency, as will be shown later, has direct repercussions on a number of fundamental rights.

[7] Ivi, 20.
[8] Roberto V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, Il Penalista, 16 January 2019.

SARI-Enterprise can be used to compare an image frame (e.g., a video from a video surveillance camera) with the A.F.I.S. database *(Automated fingerprint identification system),*[9] integrated by the S.S.A. (which stands for *Sottosistema anagrafico,* a database containing mug shots of subjects). As such, it's a form of "retrospective" FR.

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 list of provisions providing a legal basis for the data processing of the AFIS-SSA database is contained in the Decree of the Ministry of the Interior of 24 May 2017[10] and is summarised in the following table:

European level
Regulation (Eu) No 603/2013 of the European Parliament and of the Council of 26 June 2013

[9] Hermes Center for Transparency and Digital Human Rights (Laura Carrer - Riccardo Coluccini) *Technologies for Border Surveillance and Control in Italy. Identification, Facial Recognition, and European Union Funding*, 2021, 10. Available here.

[10] Decreto Ministro Interno 24 maggio 2017 recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'art. 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196, Scheda 19.

Council Decision 2008/615/JHA and Council Decision 2008/616/GAI of 23 June 2008
National level
Law 1 April 1981, n. 121
Law 23 December 1993, n. 547
Article 13, law 3 August 2007, n. 124
Law 30 June 2009, n. 85
Law 3 july 2014, n. 99
Art. 4, Consolidated text of public security laws “T.U.L.P.S.” (regio decreto 18 giugno 1931, n. 77),
Art. 7 of the regulation implementing the TULPS, regio decreto 6 maggio 1940, n. 635
Art. 11, decree law 21 March 1978, n. 59, converted into law, 18 May 1978, n. 191
Art. 5, decree law 25 July 1998, n. 286

General Application Order Concerning Biometrics - 12 November 2014 n. 513, Italian Data Protection Authority

The AFIS-SSA database contains:

A. Face images, fingerprints, and personal data of subjects who are identified by the police in the following situations:
    - Subjects who are deemed dangerous or suspicious by the public security authority and subjects who are unable or refuse to prove their identity (art. 4, Consolidated text of public security laws "T.U.L.P.S.");
    - Subjects who are under investigation (349 c.p.p.);
B. Face images, fingerprints, and personal data of individuals requesting a new or a renewed residence permit (Art. 5, c. 2-bis, legislative decree 286/1998), including those requesting international protection;
    - According to research published by Hermes, the AFIS-SSA database also includes face images, fingerprints, and personal data of migrants collected in Italian "hotspots" upon arrival on Italian soil;[11]

As argued by Hermes, "police agencies rarely explain why these individuals' facial images are already stored in the AFIS database. In some cases, it is specified that

[11] Ivi, 19. See also the video frame from an interview with a police officer contained at p. 26 which "seemingly depicts a photo identification procedure of migrants performed during disembarking operations, as specified in the Standard Operating Procedures published by the Ministry of the Interior".

the affected individuals had previously been photo-identified after committing other crimes, a detail that is however often missing in the press releases".[12]

There is no independent oversight on either:

a) the composition of the AFIS-SSA database
b) the use of SARI-Enterprise applied to the AFIS-SSA database (including its performance scores)

As such, the use of SARI-Enterprise appears to be in contrast with the principles enshrined in the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment,[13] specifically with the one of transparency.[14]

In 2018, the database "A.F.I.S.-S.S.A." contained approximately 17 million records (17.592.769 in February 2020),[15] of which 10 million were mugshots (accompanied by biographical and descriptive information).[16] The records pertained to 9.882.490 individuals, of which 2.090.064 are of Italian nationality. In the future, A.F.I.S.-S.S.A. could be integrated with other databases, such as the EURODAC ("European Dactyloscopie System"), which contains, amongst other data, the fingerprints of asylum seekers and of those who have entered or are staying

[12] Hermes Center for Transparency and Digital Human Rights, cit., 25. Hermes has submitted FOIA Requests to 22 Counter-Crime Division of 22 Italian police stations in order to inquire into "the nationalities of the people included in the database, statistical data on the use of the SARI Enterprise system and the overall number of performed searches that have led to the arrest of a suspect or have proven fruitful to the investigations", which have proven unsuccessful.
[13] Analysed below at para. 3.4
[14] Jacopo della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, Diritto Penale Contemporaneo 1/2020, 242.
[15] Parliamentary Inquiry n. 5/03482 presented by Stefano Ceccanti, 04/02/2020. Available here.
[16] See also the technical test report Sari (obtained by Riccardo Coluccini, Hermes Center for Transparency and Digital Human Rights), 9. Available here.

irregularly in the territory of the European Union.[17] According to some, such integration has already happened and explains the figure of 17 million.[18]

According to an FOI request filed by ASGI in July 2022 and sent to the Ministry of the Interior, the records contained in AFIS are now 18.460.372, of which:

- ✓ 13.516.259 belong to individuals coming from countries outside the EU;
- ✓ 1.654.917 belong to individuals from the EU (but not from Italy);
- ✓ 3.289.196 belong to Italian individuals.

2.3.1. The decisions of the Italian DPA on SARI-Enterprise and SARI-Real Time[19]

The use of SARI-Enterprise was approved by the Italian DPA in July 2018.[20] The DPA classified Sari-Enterprise as nothing but a tool which automates operations on biometric data already conducted manually by police officials on AFIS-SSA. Interestingly so, the DPA affirmed that the use of SARI-Enterprise falls under the scope of application of article 349 of the Italian Code of Criminal Procedure, which

[17] Giuseppe Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021, 240; Roberto V.O. Valli, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, cit.
The European Commission on 4 May 2016 presented a proposal to reform the EURODAC Regulation in order to allow member states to store more personal data on the database, including names, dates of birth, nationalities, identity details or travel documents, **and facial images of individuals.** The negotiations on the proposal are still ongoing and its enter into force is scheduled for April 2024 the latest. The Legislative Train Schedule can be followed here.

[18] Rita Lopez, *La rappresentazione facciale tramite software,* in *Le indagini atipiche*, A. Scalfati (ed), Giappichelli, 2019, 246, n. 11.

[19] The following chapter was written with the aid of Laura Carrer, journalist and member of the Hermes Center for Transparency and Digital Human Rights.

[20] Decision n. 9040256 of 26 July 2018. Available here.

regulates one of the most characteristic activities conducted by the judiciary police, i.e., the identification of suspects and those able to report about the course of events. Thus, it must be underlined here that "compliance with *extra codicem* regulations on the subject of privacy says nothing about the reliability and usability in the criminal trial of evidence collected through artificial intelligence algorithms",[21] such as SARI-Enterprise. The topic will be examined in the following paragraph.

The use of SARI-Real Time, instead, was subject to a decision of the Italian DPA in March 2021.[22] The DPA stated that such a module entails **new processing of biometric data,** which is **ontologically different from video surveillance, and, as such, its approval was denied as lacking an appropriate and specific legal basis.** Specifically, the DPA affirmed that the Ministry of the Interior did not satisfy the requirements imposed by Article 7 of Legislative Decree 18 May 2018, n. 51. Legislative decree n. 51/2018 implemented the Law Enforcement Directive ("LED")[23] in Italy. As will be further explained below, Article 7 Legislative Decree 51/2018 explicitly mandates that the processing of data referred to in Article 9 of the General Data Protection Regulation ("GDPR"), which includes biometric data, is authorised only if strictly necessary and assisted by appropriate safeguards for the rights and freedoms of the data subject **and specifically provided for by European Union law or by law or,** in cases provided for by law, **by regulation**, or, without prejudice to the safeguards for the rights and freedoms, if it is necessary

[21] Marco Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale,* Diritto penale e processo 8/2021, 1052.
[22] See Decision n. 9575877 of 25 March 2021. Available here.
[23] 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. See para 4.6.

to safeguard a vital interest of the data subject or another natural person or if it relates to data made manifestly public by the data subject.[24]

Indeed, the Ministry of the Interior, in its request for the pre-emptive approval of the use of SARI-Real Time to the DPA (specifically, in the Data Protection Impact Assessment, "DPIA"),[25] had indicated numerous articles of the Code of Criminal Procedure as a possible legal basis for such data processing activity. The legal base indicated was then deemed insufficient by the DPA in its decision of March 2021.

The table below summarises the articles mentioned by the Ministry of the Interior and the arguments of the DPA:

Art. 134 co.4 (documentation of the proceedings by audio-visual reproduction)	These articles concern, respectively, the documentation of acts by audiovisual reproduction, the acquisition of writings or other documents by photography, cinematography, phonography, and other means, the interception of communications between persons present by means of portable
Art. 234 (acquisition of writings or other documents by	

[24] Moreover, the Italian DPA specified that "The identification of a person would be achieved by processing the biometric data of all those present in the monitored space in order to generate patterns comparable with those of the individuals included in the 'watch-list'. This would result in **an evolution of the very nature of surveillance activity, marking a shift from targeted surveillance of certain individuals to the possibility of universal surveillance**". In this regard, see the decisions *Centrum för Rättvisa v. Sweden* (2021) and *Big Brother Watch and others v. the UK* (2021) reported at para 3.2.

[25] A Data Protection Impact Assessment (DPIA) is a procedure that identifies risks associated with the processing of personal data and seeks to mitigate them as much as feasible in advance. DPIAs are crucial instruments for reducing risk and proving GDPR compliance. Under the GDPR, DPIAs are mandatory for any new high risk processing projects.

photography, cinematography, phonography and other means)	electronic devices, and the interception of telematic communications streams. According to the Italian DPA's decision on SARI-Real Time, **these provisions do not provide a suitable legal basis for the processing of biometric data aimed at personal identification via SARI-Real Time.**
Art. 266 (Wiretapping of communications between individuals by means of portable electronic devices)	
Art. 431 co. 1 lett. b. (Composition of the "file" for the adjudication phase of the trial)	
Art. 55 (Functions and duties of the judicial police)	These articles pertain to the functions of the judicial police in securing sources of evidence and conducting investigations of places or persons, on the initiative or by the delegation of the judicial authority, but they do not provide for the processing of biometric data, so they do not constitute a legal basis which is capable of satisfying the threshold established by Article 7 of the Legislative Decree 51/2018. Hence, they cannot justify the use of SARI-Real Time.
Art. 348 (Judicial police and securing sources of evidence)	
Art. 354 (Urgent inspections of places, things and persons. Seizure)	
Art. 370 (Competencies of the public prosecutor - Direct and indirect competencies of the judicial police)	

Let us now take a step back, specifically to before the DPA issued its negative opinion on SARI-Real Time.

It is interesting to notice, as it was reported by Hermes, that the Ministry of Interior "had published a public contract notice for an upgrade to the *[SARI-Real Time]*

system, to be used for monitoring the landing of migrants and asylum-seekers on Italian shores"[26] much before receiving a deliberation by the DPA.

Indeed, since May 2020, the Department of Public Security, under the Central Anti-Crime Directorate of the Ministry of the Interior, has begun to explore possible enhancements to the SARI facial recognition system supplied, both in its Real-Time and Enterprise versions. The first exploratory notice,[27] dated 25 May 2020, launched a market survey to understand the reference market. The enhancement was related to the FR algorithms of the SARI-Enterprise system. With regard to the real-time mode, however, in the exploratory notice, the Anti-Crime Department made clear reference to the strengthening of the system also by virtue of the need to "monitor the disembarkation operations [of migrants] and all the related illegal activities, video-record them and identify the subjects involved". It is also specified how the enhancement could not be assigned to other companies except Parsec 3.26 s.r.l., i.e. the same that had created the system for law enforcement in 2017.

On March 3, 2021, twenty days before the negative opinion of the DPA, the tender of the enhancement of the Sari system to the company Parsec 3.26 was published in the Official Gazette.[28] In fact, it seems that the system has been enhanced,

[26] Hermes Center for Transparency and Digital Human Rights, cit., 11.

[27] Polizia di stato, Avviso esplorativo, ex art. 66, comma 1, del d. lgs. n. 50/2016, finalizzato alla partecipazione ad una procedura negoziata senza previa pubblicazione del bando di gara per l'approvvigionamento di apparecchiature hardware e software finalizzate a potenziare le attuali funzionalità e prestazioni delle due componenti del sistema automatico riconoscimento immagini (SARI), denominate: SARI Enterprise e SARI Real-time, in uso alla direzione centrale anticrimine nell'ambito del progetto "falco extended" (progetto n. 87.5.1) - fondo sicurezza interna 2014- 2020. Available here.

[28] Ministero dell'Interno, Esito di gara-Procedura negoziata senza previa pubblicazione del bando di gara per l'approvvigionamento di apparecchiature hardware e software finalizzate a potenziare le attuali funzionalità e prestazioni delle due componenti del Sistema Automatico Riconoscimento Immagini (SARI), denominate: SARI Enterprise e SARI Real-Time, in uso alla Direzione Centrale Anticrimine CUP F89D19000100006 - CIG 85092230F6, 70. Available here.

nevertheless, in the Real-Time part, this enhancement has never actually been used by the police (*Polizia di Stato*).

Thus, on the same day, in response to a parliamentary inquiry, the Ministry of the Interior declared:

> "SARI Enterprise is a software that can be used exclusively by operators of the State Police and the Carabinieri, after specific training and qualification. The images are captured both by Police offices, which conduct investigations related to criminal proceedings and by the Service for International Police Cooperation of the Central Directorate of the Criminal Police within the scope of activities of their specific competence. [...] **The SARI system is not in use as part of the activities of the Central Authority on Immigration and Border Police** *[Direzione centrale dell'immigrazione e della polizia delle frontiere]* and does not have different domains depending on the subjects (Italian citizens, migrants, etc.), but rather **is a system that will operate indiscriminately** when fully operational, in support of investigative activities."[29]

According to Hermes,

> […] **the indirect effects of biometric surveillance are liable to affect migrants and asylum-seekers regardless since their facial images are stored in a database used in combination with the SARI Enterprise facial recognition system**. This makes the criminalisation of foreign

[29] Filippo Sensi, interrogazione a risposta immediata "Intendimenti in ordine all'utilizzo di sistemi di riconoscimento facciale, anche in relazione alla necessaria tutela dei diritti fondamentali della persona – n. 3-02074. Available here.

> nationals ingrained within the Italian technological infrastructure: **biometric data collected during landings are included in a database that contains data about individuals that have been investigated (but not convicted**). Without proper oversight of the use of this system, there is a concrete risk of producing false positives and violating the rights of certain categories of particularly vulnerable people.[30]

And what about what happened *after* the negative decision of the DPA on SARI-Enterprise? It seems as though the interest of law enforcement in FRTs was not hindered by the DPA's opinion.

As a matter of fact, in October 2021, the general command of the *Arma dei Carabinieri* published a notice of tender[31] aimed at acquiring 4 FR systems for the operational needs of various departments of the Carabinieri. The total value of the contract was 82,000 euros, an offer proposed by ECUBIT s.r.l. Unfortunately, it was not possible to find any other document about the tender and therefore not even the technical requirements required by the Carabinieri for the functioning of the system or the reasons behind the purchase. This aspect is particularly relevant if we think that the tender procedure was a negotiated procedure, i.e., a procedure through which "the contracting authorities consult the economic operators they have chosen and negotiate the contract conditions with one or more of them".[32] Moreover, the Ecubit s.r.l company website does not provide information about the FR systems it produces. In total, for the four facial recognition systems and

[30] Hermes Center for Transparency and Digital Human Rights, cit., 34.

[31] Comando Generale dell'Arma dei Carabinieri, Approvvigionamento n.4 sistemi "Face Recognition" per le esigenze operative dei Reparti dell'Arma dei Carabinieri-Avviso aggiudicazione appalto. Available here.

[32] Art. 3, paragraph 1, Legislative Decree n. 50/2016.

software licences, the Carabinieri declared that they had incurred an expense of 100,040 euros.[33]

Furthermore, the general command of the *Guardia di Finanza* published, at the end of May 2021,[34] a letter of invitation to companies to develop a biometric capture software product and related source code for photo signaling. The contract was awarded to Almaviva s.p.a for the value of 298,000 euros.

On a final note, it must be highlighted that the Italian DPA also dealt with **Clearview AI, a company that offers FR-based search on images freely accessible on the web to public authorities**. The proceedings arose from press reports denouncing the critical aspects of Clearview AI's data management, and from four complaints from individuals who had discovered that the company held several images of them without their consent. The DPA found Clearview's activities to be contrary to the provisions of the GDPR concerning the principles that must characterise data processing (fairness and transparency, purpose limitation and limitation of storage); the conditions of lawfulness of the processing in general and those laid down for particular types of sensitive data, as well as the provisions concerning the respect of the rights of the data subject. Therefore, it ordered the application of an administrative pecuniary sanction of twenty million euros.[35] As reported in an investigation conducted in 2021 by BuzzFeed News,[36] the Italian *Polizia di Stato* made use of Clearview's services by running 130 searches.[37]

---

[33] Comando Generale dell'Arma dei Carabinieri - Pagamenti 1° Trimestre 2022. Available here.
[34] Guardia di Finanza, Acquisto di un prodotto software per il foto-segnalamento e servizi correlati. Available here.
[35] Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Clearview AI, provvedimento n. 50 del 10 febbraio 2022.
[36] Read the article here.
[37] Clearview AI was also addressed by other DPas. The *Commission nationale de l'informatique et des libertés* ("CNIL"), the French DPA, found in its investigation that Clearview AI was in breach of several sections of the GDPR including article 6 which is the unlawful processing of personal data because the collection and use of biometric data were carried out without a legal basis.

Finally, according to the recently adopted moratorium, which will be discussed below in paragraph 2.4, one must underline that judges and prosecutors could order the instalment of a real-time FR system, without the *Garante's* prior authorization, notwithstanding the negative opinion of the Garante on SARI-Real Time. This is valid until the cease of validity of the moratorium, which is set for December 31, 2023 (unless specific regulation is implemented before). When it comes to LEAs, nothing changed, in the sense that they cannot use real-time FR, only static.

Furthermore, in breach of articles 12, 15 and 17 of the GDPR, it failed to take into account the rights of individuals in an effective and satisfactory way, specifically in terms of requests for access to their data. In fact, Clearview collected and used people's photos without their permission in order to supply its software. Given the intrusive and extensive nature of the process, Clearview AI did not have a legitimate purpose in collecting and utilising this data either. These persons do not reasonably expect their images to be processed by the corporation to provide a facial recognition system that could be utilised by States for law enforcement reasons, despite the fact that their photos or videos are available on several websites, including social media.CNIL, *Facial recognition: 20 million euros penalty against CLEARVIEW AI*, 2022. Available here. On the same matter, the Swedish Authority for Privacy Protection also concluded that the Police had not complied with its obligations as a data controller on a number of fronts. The Police did not put in place enough organisational safeguards to guarantee and be able to show that the processing of personal data in this case complied with the Criminal Data Act. Using Clearview AI for facial recognition, the Police handled biometric data in an unauthorised manner and neglected to undertake the necessary data protection impact assessment. Swedish Authority for Privacy Protection, Police unlawfully used facial recognition app, 2021. Available here. Similar decisions have been adopted by the UK's Information Officer (ICO); by the Office of the Australian Information Commissioner (OIAC) and by the Hellenic Data Protection Authority (HDPA).

2.3.2. The use of SARI-Enterprise vis-a-vis the rules on evidence contained in the Italian Code of Criminal Procedure

The questions that arise relate to how the outputs of an FRT could enter the criminal law trial and to whether they could be used as the predominant (or only) evidence for the application of a pre-trial measure or for a conviction.

The issue is more than topical at the moment. By way of example, one can mention the interdisciplinary group "AI 4 Intelligence", funded by the Dutch Research Council (NWO), which is researching issues of how to translate AI-generated information "into admissible court evidence"[38] in a way that it is compliant with "the general evidentiary requirements of reliability and lawfulness". Specifically, the researchers will look into two questions:

> First, there is a lack of (clear) rules as to how the evidentiary requirements – developed for analogue situations with different types of evidence in mind – are to be operationalised in the context of AI in the criminal process. And, second, AI diminishes the transparency and explainability of the evidence-creation process. The resulting effect reduces the possibility of the judge and the defence to question and contest AI-generated evidence (i.e., 'contestability'). The end result is that neither the judge nor the defence can properly assess whether the content of the information is truthful and has been obtained through legal methods. The lack of contestability of AI-generated evidence therefore has a significant effect on one of the core rights and principles of the criminal process: the right to a fair trial and the accompanying principle of equality of arms.[39]

[38] See the recent call for a PhD researcher published by Vrije Universiteit. Available here.
[39] Ibid.

When it comes to the Italian case, we can identify two main issues in this regard**:**

1. whether the output produced by an FR system, such as SARI-Enterprise, could qualify as a **new form of scientific evidence,**[40] and therefore could "enter" the criminal trial via art. 189 of the Code;
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.

Let us focus now on n.1.

As was already highlighted, article 189 of the Italian Criminal Code refers to evidence not regulated by law. The admissibility of such evidence is subject to the discretion of the judge, who must determine if its inclusion is appropriate to establish the facts of the case, while also not impinging upon the individual's moral autonomy. The judge will make a ruling on the admission of this evidence after hearing the arguments presented by the parties regarding its admissibility.[41]

As of today, there are no *codified* rules on the admission and evaluation of "new" scientific tools as evidence in a criminal trial in Italy. The general issue has been dealt with by courts, such as the *Via Cozzini* judgement,[42] which identified a set of criteria suitable for assessing the **admissibility** of scientific evidence, i.e., for

[40] Valli, cit.

[41] It has been argued that art. 189 "deploys a useful test, measuring effective demonstrative potential of an automatedly generated evidence. In advocating such demonstrative potential, parties are forced to elaborate upon the transparency and the explainability of the automated process that generated the information that they want to use as evidence. Thus, an adversarial debate can arise between defense and prosecution". Gialuz & Quattrocolo, cit., 25.

[42] Cass. pen., Sez. IV, 17 September 2010, n. 43786.

verifying the validity and reliability of such evidence in order to rule on its entry in the trial (e.g., general acceptance, peer review, publication, the margin of error,…).

As it was argued,

> The Supreme Court, especially when called upon to pronounce on the subject of new scientific methodologies posed as the basis for the application for trial review [*revisione*], in fact, tends to limit the scrutiny of the reliability of scientific evidence to the verification that **it has been recognized by the relevant scientific community** (Cass. pen., 8 marzo 2011, n. 12751, Cutaia; Cass. pen., 4 luglio 2013, n. 34531, Mazzagatti; Cass. pen., 14 novembre 2017, n. 16751, Cirocco). If we now go on to examine the case of Sari, we find that **the search parameters by which the system operates have not been made public, the tests carried out regarding the actual recognition ability of the faces analysed are not known, the rates of false positives and false negatives are not known, and how the validation of the system was carried out (size of the test sample, procedure used to measure the accuracy of face prediction) is not known;** in this context, both because of the absolute novelty of the system and especially because of the lack of knowledge of the elements now indicated**, it is understandable how a consensus of the scientific community on the validity of the method used has not even been formed.**[43]

Moreover, in the field of FR "[i]n play, in particular, is the so-called principle of non-substitutability, under which it is not possible to circumvent the substantive rules

[43] Valli, cit.

and guarantees provided for the typical act by fraudulently qualifying it as atypical; a principle for the protection of the rule of law that informs the evidentiary system, or of the task recognized to the law of outlining the limits of the what and how in an attempt to balance the openness of the criminal procedure to the use of the most modern technological means with the absence of explicit regulations."[44]

It follows that one could admit the use of SARI, and similar FRT, as mere investigative tools, but that the same should not be qualified as evidence according to the Italian Criminal Code of Procedure.[45]

Let us focus now on n.2.

In this context of technological innovation in the field of personal identification, SARI could represent the new frontier of the investigation activity referred to as "photographic identification".[46]

According to some,[47] the use of SARI-Enterprise could be reconducted to the practice of "photographic recognition" (*ricognizione fotografica*) conducted by the judicial police,[48] which is considered an "atypical product" of the "typical" act of investigation referred to in art. 361 of the Italian Code of Criminal Procedure.

[44] Mobilio, cit., 86.
[45] Ibid.
[46] Lopez, cit., 253.
[47] Ernestina Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, Legislazione Penale, 2020, 14; Lopez, cit. 246.
[48] During the investigation phase, the police can create an album of pictures which contains the picture of the suspect(s) and of other individuals. The album is then shown to the victim/witnesses to test whether they recognize anyone.

Art. 361 of the Code of Criminal Procedure regulates the identification of people, things, or anything else that may be the object of sensory perception (e.g., smells or voices). The article explicitly prescribes (II c.) that identification can be conducted through the act of showing an individual a picture of the person or the object. Such activity does not constitute *evidence* per se, in the sense that it cannot be used by a judge in their reasoning on the blameworthiness of an individual. It is rather conceived as a tool which could be used by the prosecutor to guide their investigations.

Nevertheless, according to jurisprudence, photographic identification represents a type of **atypical evidence** and, as such, it can enter the criminal trial under Article 189 of the Code of Criminal Procedure if the judge deems it suitable to ensure the establishment of facts.[49] Specifically, according to case law, the reliability of such identification derives not from the recognition per se, but from the reliability of the person who, by deposing and examining the photo, says they are certain of the identification they are making.[50]

It follows that if the judge rules that such atypical evidence is admissible, it will be able to use it to prove the facts, provided that the credibility of the person who, when identifying, said they were certain of the identification made, is established. The identification can be conducted by the prosecutor or by the police (both upon express order from the prosecutor and of its initiative during an investigation).

On this matter, it has been argued, if we were to consider facial recognition as a "species [...] of the genus photographic identification performed by the judicial police, the obvious and fundamental element of distinction resides in the **nature**

[49] See Cass.pen., sez. V, n. 22612/2009; Cass. pen., sez II, n. 29847/2016.
[50] See Cass. pen., sez. VI, n. 49758/2012.

of the identifier: in the first case, a 'machine', in the second, the human person - the offended person or a person informed of the facts."[51] As such, it might well be that the results of the recognition conducted by an automated system outperform those conducted by humans[52] - even though, in the specific case of SARI, as it will be further highlighted, the Ministry of the Interior has not disclosed any data on the quality of its results.

Surely, the use of SARI will have to comply with the principles of due process, as established not only at the constitutional level but also at the European and international one. Most notably, the Italian legislature and government will have to take into consideration the development of soft law instruments on the matter, such as the Council of Europe ("CoE") "European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment".[53]

It has been argued that "S.A.R.I., to date, offers few reliable guarantees of compliance with the 'significant methodological precautions' that the European Union recommends to ensure the transparency, quality and external verifiability of the procedures used."[54] Specifically, it is questioned how the defence will be able to "rebut the identification of the suspect as the outcome of an analysis that, by its inherent characteristics, is inaccessible."[55]

Indeed, it is the obscurity of the functioning of this system which "precludes any attempt to falsify the relevant result in cross-examination."[56] As a consequence,

[51] Lopez, cit., 255.
[52] Ibid.
[53] See below at para 3.4.
[54] Lopez, cit., 256.
[55] Ivi, 257.
[56] Ibid.

the only possible object of cross-examination if the output of SARI were to enter the criminal trial as evidence, would be a "mediated source", i.e., "the forensic police report illustrative of the verification of the reliability of the output, through the classical identification standards, based on discriminatory parameters that are both metric (e.g., eye distance, cheekbone height, mutual position between nose and mouth, etc.), as well as physiognomic (face shape, nasal pyramid, auricle, mouth shape, jaw branch, chin protrusion, hairline point shape of eyes and eyebrows, etc.)."[57] As a result, the cross-examination of the results of SARI appears to be impossible, hence in contrast with the principle of due process.[58]

Finally, under Italian law, there are no rules on whether FRT can be used only for investigation activities related to specific types of crimes, nor is there any specific regulation on the duration of the use of said technologies.

But what is the *actual* use of FRT by law enforcement and judicial authorities in Italy?

As it was mentioned above it comprises – so far – "only" SARI-Enterprise, so *retrospective* FR.

As of today, **there has been no Italian case law specifically on SARI.**[59] In September 2018, the Italian police (*Polizia di Stato)* reported on its website that it

[57] Ibid.

[58] Sacchetto, cit., 14. Although the US is a distant system from the Italian one, scholars have started canvassing techniques to challenge FR in (criminal) court. See for example: Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Cour*t, The Champion, 2019. Available here; Rebecca Darin Goldberg, *You Can See My Face, Why Can't I? Facial Recognition and Brady,* Columbia Human Rights Law Review, 2021. Available here.

[59] Other relevant (non Italian) national case law includes the decision on the use of FR by the South Wales Police, on 11 August 2020. In the absence of specific legislation governing the use of TRFs by police forces, the Divisional Court claimed that the specific use of the software "AFR Locate"

had arrested two suspects of Georgian nationality accused of a theft committed in an apartment in Brescia[60] thanks to a match found by SARI-Enterprise in the AFIS-SSA database using frames taken from video surveillance recordings of the location of the crime. In August 2021, a national newspaper reported that the police were able to identify a subject of Egyptian nationality guilty of rape thanks to his WhatsApp profile picture. SARI-Enterprise matched said image with the one taken upon his arrival in Italy via the Lampedusa island and with the one taken upon his request for international protection at the immigration offices in Milan.[61] In January 2023, it was reported that the Police used SARI-Enterprise to identify a suspect guilty of attempted murder of a young tourist at the station of Roma Termini thanks to the videos recorded by the cameras present in the station. The suspect, of Polish nationality, was already present in the AFIS-SSA database since they had been identified (and photographed) by the police a few days earlier in relation to the commission of a theft in a bar.[62]

The only mentions of the SARI system in criminal proceedings by a Court date back to a decision of the Italian *Corte di Cassazione* of 2020.[63] Even though the judgement relates to a procedural matter concerning the notice of the date of a hearing (i.e., the violation of art. 606 of the Code of Criminal Procedure) it is relevant as it **explicitly mentions the use of SARI-Enterprise during investigations**.

falls within the "common law powers" of the Welsh police (R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341 (Admin), p. 78). The Court of Appeal reversed the judgement and affirmed that its use was unlawful and violated the ECHR (art.8) and UK data protection law.

[60] Read the news here.

[61] Read the news on Corriere della Sera Milano here.

[62] Read the news on Repubblica here.

[63]; Cass. pen. sez. I, n. 21823/2020.

A public prosecutor in Milan used SARI-Enterprise to identify the faces of five subjects involved in a brawl which were recorded by a video surveillance system present on a scene and a video made by a person present at the time. As stated *obiter dictum* by the *Corte*, **the faces recorded in the video frames were compared to those faces "present on telephone accounts of people involved in the event".** Notice here how the words "faces present on telephone accounts" are used to translate the Italian phrase "*effigi presenti su utenze telefoniche*". The phrasing is puzzling and it is our understanding that it is used to refer to profile pictures on WhatsApp accounts.

The use of SARI-Enterprise led to one match which was then used by the prosecutor to request the application of a pre-trial detention measure on an individual "B". The request was denied by the Judge of Preliminary Investigations of Milan and its decision was confirmed by the Court of Review (*Tribunale del Riesame*) since "the images used for the facial recognition were not clear and didn't allow for recognition of the facial traits, clothes worn or specific traits of the attacker, for which no hard evidence could be found."[64]

Finally, it can be argued that SARI-Enterprise can play different roles in the Italian criminal trial. First, it can be used as a "pre-investigative tool,"[65] i.e., as part of the activities carried out by the police before the prosecution charges a suspect (hence before a suspect is formally accused of a crime). It can also be used as an investigative tool by the prosecutor in order to steer his investigation and, as such, be subsumed in the already-existing 'traditional' identification systems provided for in the Code of Criminal Procedure.[66] Finally, in the future, it could enter the criminal

[64] Ibid.
[65] Luisa Saponaro, *Le nuove frontiere tecnologiche dell'individuazione personale*, Archivio Penale n. 1/2022, 4.
[66] Ibid.

trial as evidence and, as such, be treated as atypical evidence according to article 189 of the Code. It is debated whether it would constitute a new type of scientific evidence, or whether it could be assimilated into photographic identification (article 361, c.2 of the Code), which, as mentioned above, is considered evidence according to the dominant case law. Surely, the most problematic aspect lies in the fact that the opacity of SARI, both regarding the functioning and the performance of its algorithms, and the composition of the AFIS-SSA database, hinders the possibility for the defence to contest its admission as evidence in trial.[67]

2.4. Focus: uses of "biometric surveillance" by local administrations (*Comuni, Regioni, …*)[68]

2.4.1. The case of Como

It often happens that political choices, and consequently spending choices, are not advertised or defined together with the local population. And so it was for the FR system implemented by the municipality of Como in 2019. The document containing the public works to be carried out in the two-year period 2020-2022 also envisaged the acquisition of an intelligent video surveillance system equipped with FR, in order to monitor what was happening in the square of the central station of Como and the nearby park Tokamachi. In 2016, the city had been affected by a substantial flow of immigration directed towards Switzerland, which however did not welcome migrants, causing them to stay in the square and park of the Como station.

[67] Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale,* cit., 1053.
[68] The following chapter was written with the aid of Laura Carrer, journalist and member of the Hermes Center for Transparency and Digital Human Rights. Her full investigation is available here.

At that time, the municipality of Como, governed by a *Lega Nord* mayor close to the then minister of the interior Matteo Salvini, made urban security a bulwark for its local politics. The FR system was largely celebrated as the solution, according to the municipal administration, to the continuous arrival of migrants at the border with Switzerland, a cause of disturbance for the citizens of Como.

The FR system had been bought by Huawei Italy, after various meetings with municipal and company representatives, through a procedure below the threshold (less than 40,000 euros) and was able to identify "black, yellow, white people". The municipality had not carried out any preventive impact assessment for the use of the system, and the investigation revealed that it was not aware of the type of tool it had purchased and intended to use.

In March 2020, during the drafting of the investigation, Wired proceeded to inform the DPA of what was happening: the latter ordered the municipality to provide explanations.

In this regard, in response to a parliamentary inquiry on the matter of June 10, 2020, presented by Deputy Filippo Sensi (n. 4/05966) the Ministry of the Interior declared that the activities conducted by the Municipality of Como were justified by the following legal basis, specifically directed to the use of FR systems by local entities:

- Art. 5 c. 2. a), d.l.14/2017 (converted into law n. 48/2017) which identifies, among the tools for preventing and combating phenomena of widespread crime, within the framework of the "covenants for the implementation of urban security" signed between the prefect (*prefetto*) and the mayor, the use of urban video surveillance systems, which can be implemented by

local authorities, also using state resources provided by the same law, as a result of a specific competitive procedure defined by an interministerial decree;

- More sources that are mentioned:
    - Linee generali delle politiche per la promozione della sicurezza integrate, 24 January 2018;
    - Linee guida per l'attuazione della sicurezza urbana, 26 July 2018;
    - Direttiva Ministero dell'Interno "Sistemi di videosorveglianza in ambito comunale", 2 March 2012;
    - Italian DPA's "Act on Videosurveillance", 8 April 2010 (which, questionably, is qualified as "the point of reference in relation to the important privacy profiles"),

All these sources refer to mere video surveillance activities, they do not mention the processing of biometric data, hence they are not relevant.

In February 2020, the Italian DPA, having verified the lack of a legal basis for the use of the system (as well as of the possible violation of the right to privacy of citizens of Como and beyond), ordered the cameras to be turned off. The DPA's decision of February 2020 can be summarised as follows:

- the processing of biometric data for purposes of "preventive protection of urban security"[69] conducted by local authorities (ex art. 4 of Decree-law

[69] The concept of "urban security" for d.l. 14/2017 is defined in art. 4 of the same decree as "The public good that relates to the livability and dignity of cities, to be pursued through redevelopment efforts, including urban, social, and cultural initiatives, and the recovery of degraded areas and sites, the elimination of factors of marginalization and social exclusion, the prevention of crime, especially predatory crime, the promotion of a culture of respect for the law and the achievement of higher levels of social cohesion and civil coexistence, to which the State, the Regions and autonomous Provinces of Trento and Bolzano and local authorities contribute primarily, also through integrated interventions, in accordance with their respective competencies and functions".

14/2017) can be qualified as "investigation activity" done by law enforcement according to article 349 of the Code of Criminal Procedure[70] - as it was also stated with regards to SARI-Real Time - and, as such, it falls within the scope of the application of art. 7 of d.l. 51/2018;

- Nevertheless, art. 6, c. 6 Decree-law 11/2009, which states that "Municipalities may use video surveillance systems in public places or places open to the public" to safeguard urban security does not qualify as an appropriate legal basis for the processing of biometric data (as requested by art. 7 d.l. 51/2018).

The case has certainly also brought to light a second aspect, relating to how public administrations spend public money. It was not such a high amount, but, in any case, public finances were used to purchase technological tools that had no (and still have no) legal basis to be implemented, and which began discussions a few months later in the European Union.

2.4.2. The case of Turin

In August 2020, the municipal council of Turin discussed possible financing of the "ARGO" project through the ministerial funds on the urban security foreseen for the municipalities for the year 2020 (17 million euros): the Municipality allocated 800,000 euros, the Ministry of the Interior 700,000. The preliminary project was defined and assigned to the company 5T s.r.l., a public company that controls mobility in Turin, with a total financing of 1,500,000 euros.

The two phases of the project would first involve the peripheral area, which will also include the management of the video surveillance systems created as part of

[70] Specifically identification of subjects who are under investigation or who posses information on facts relevant to a criminal investigation.

the AxTO project (which already favoured the so-called "participatory surveillance"), and, second, the central area of the city. The project was finalised in October 2020, and the company 5T s.r.l. received the first instalment for the first phase of ARGO, which was scheduled to start in January 2021.

The ARGO project aimed to integrate tools for monitoring mobility and traffic with city video surveillance systems. The final design document states that the system will be able to extract real-time metadata from videos. If the word metadata may not say much, the examples indicated by the local police and by the company 5T, in charge of carrying out the work, are instead very clear. They are the “distinction between man/woman; the colour of clothing and shoes; the presence of objects such as bags, backpacks, hats, etc”. With this type of information it would be possible to identify and follow people filmed in real-time: a hat, a red bag or a simple shirt with a logo, combined with information on the person's gender, allow one to follow a person’s movements perfectly.

The Hermes Center obtained, thanks to various FOIA requests, a copy of the final project approved by the Council on 26 October and various previous versions, the first dating back to June 2018.[71] In 2018, the municipality had to redact a DPIA in order to assess the risks to individual rights linked to the use of the system. For the following two years, the municipality always replied to Hermes Center stating the document was still being finalised. This is the reason why in January 2021 Hermes reported the case[72] to the DPA in which it asked for the Argo project to be taken over and analysed in depth, to understand possible risks of violations of privacy and human rights.

[71] They are all available here.
[72] The notice is available here.

With the ARGO project, the municipality of Turin introduced a widespread video surveillance network aimed to "control urban security, integrated security and mobility governance," which adds to the video cameras already installed previously. Such a system would include features such as line crossing detection (detection of crossing a predefined line), intrusion detection (detection of intrusions in a certain area), region entrance (detection of the entry of a person/vehicle in a predefined region), region exiting (the opposite of above) and motion detection (detecting the movement of a person/vehicle). The cameras in the city are expected to be 360.

After the negative opinion of the DPA on the similar Como project, and the introduction of the moratorium on facial recognition at the end of 2021, the Turin-based Argo project came to a stop. In January 2023, after years of stalemate, the newspaper La Stampa reported[73] the change of mind of the municipality: **the video surveillance system will not have facial recognition algorithms on board.**

During the publication of the investigation on the municipality of Como, the Hermes Center looked for other cases of the adoption of similar FR systems. The research was unsuccessful. However, it is presumed that before the DPA took charge of the situation, and before the moratorium on facial recognition, other municipalities also had at least thought of buying similar systems. **It is for this reason that StraLi is now conducting new research, addressed both at municipalities and at police headquarters.**

On November 17, 2021, Deputy Sensi presented another parliamentary inquiry to the Ministry of the Interior, this time related to an AI-based video surveillance

[73] Read the article here.

system purchased by the municipality of Pescara[74] (the system is the result of an investment of 1,404,392 euros, of which about 904,392 were financed by the Ministry of the Interior) which comprises more than 332 ultra-high resolution cameras positioned in 34 strategic areas. The system offers the possibility of performing a predictive analysis, based on certain levels of alarm, and can be integrated with third-party facilities (private parties, for example, such as shopkeepers). **The parliamentary inquiry was left unanswered.**

Finally, there is no doubt that the case of Como told through the investigation published on Wired Italia was the spark that brought the attention of the authorities and in part also of the public to facial recognition systems. The Reclaim your Face campaign, which began in late 2020 and continued until summer 2022, of which StraLi was an active participant, aimed for a ban on facial recognition systems in the cities. Even if it did not reach 1 million signatures in Europe, the campaign definitively drew political attention to the issue, at the European and Italian levels, leading to the adoption of the moratoriums in various European countries including Italy, as it will be analysed in the following paragraph.

2.5. The moratorium

Following the European Parliament Resolution of 6 October 2021 on the use of AI in criminal law, Italy effectively approved a moratorium on FR systems in public places or places open to the public until the end of December 2023, with the exception, **however, of the processing carried out by "competent authorities" for the purposes of preventing and repressing crimes or executing criminal**

[74] See the news here.

sanction according to Legislative Decree 51/2018 (which, as mentioned above, implemented the LED Directive in the Italian legal system)**.** The moratorium was adopted with Law 3 December 2021, n. 205.[75]

The adoption of the moratorium has been controversial, as it "shows clear lack of awareness about the different levels of complexity in this matter."[76] One of the main criticism is that the notion of "competent authorities", i.e., subjects that are competent to carry out actions directing at the prevention and repression of crimes, includes public administrations. It follows that according to some authors even local municipalities ("*Comuni*") could make use of the exclusion to the moratorium and would therefore be able to install video surveillance systems which include FRT.[77]

The most important articles of the law implementing the moratorium are mentioned in the following table:

Article 9	
ITALIAN TEXT	**ENGLISH TEXT**

[75] Conversion of decree law 8 October 2021, n. 139 containing urgent provisions for access to cultural, sports and recreational activities, as well as for the organization of public administrations and on the protection of personal data.
[76] Mitja Gialuz & Serena Quattrocolo, *AI and the administration of Justice in Italy,* e-Revue Internationale de Droit Pénal, 2023, 24. Available here.
[77] Ernestina Sacchetto, *Riconoscimento Facciale, l'approccio Italiano è in Antitesi Alla Ue: I Nodi,* Agenda Digitale (blog), 7 December 2022. Avaialble here.

9. In considerazione di quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea, l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023.	9. In view of the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, as well as Directive (EU) 2016/680 of the European Parliament and of the Council, of April 27, 2016, and the need to regulate in accordance with the eligibility requirements, conditions and safeguards relating to the use of facial recognition systems, in compliance with the principle of proportionality provided for in Article 52 of the Charter of Fundamental Rights of the European Union the installation and use of video surveillance systems with facial recognition systems operating through the use of biometric data referred to in Article 4, number 14), of the aforementioned Regulation (EU) 2016/679 in public places or places open to the public, by **public** authorities or private entities, shall be suspended until the entry into force of legislative regulation of the matter and in any case no later than December 31, 2023.

Article 11	
ITALIAN TEXT	**ENGLISH TEXT**
11. In caso di installazione o di utilizzazione dei sistemi di cui al comma 9, dalla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2023, salvo che il fatto costituisca reato, si applicano le sanzioni amministrative pecuniarie stabilite dall'articolo 166, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e dall'articolo 42, comma 1, del decreto legislativo 18 maggio 2018, n. 51, in base al rispettivo ambito di applicazione.	11. In the event of installation or use of the systems referred to in Paragraph 9, from the date of entry into force of the law converting this decree and until December 31, 2023, unless the act constitutes a crime, the administrative pecuniary sanctions established by Article 166, Paragraph 1, of the Code referred to in Legislative Decree No. 196 of June 30, 2003, and Article 42, Paragraph 1, of Legislative Decree No. 51 of May 18, 2018, shall be applied, according to their respective scope of application.
Article 12	
ITALIAN TEXT	**ENGLISH TEXT**
12. **I commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e**	12. **Paragraphs 9, 10, and 11 do not apply to processing carried out by the competent authorities for the purposes**

repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, **in presenza**, **salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero,** **di parere favorevole del Garante** reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018.	**of preventing and repressing crimes or executing criminal sanctions** referred to in **Legislative Decree No. 51 of May 18, 2018**, in the presence, **except in the case of processing carried out by the judicial authority in the exercise of judicial functions as well as judicial functions of the public prosecutor**, **of a favourable opinion of the Italian Data Protection Authority** rendered pursuant to Article 24, paragraph 1, letter b), of the same Legislative Decree No. 51 of 2018.

The **moratorium** has (almost) **no effect on the activities regulated by d. lgs. 51/2018**, i.e., the processing of personal data for prevention, investigation, assessment, and prosecution of crimes or execution of criminal sanctions, including those aimed at the safeguarding and protection of threats to public safety.

Indeed, according to the text of art. 9 para 12 of law 205/2021, both law enforcement and judicial authorities (including prosecutors) are exempted from the suspension on the installation and use of FR systems. Thus, the former (i.e., LEAs) are still obliged to seek the prior (binding) opinion from the Italian DPA, whereas the latter (i.e., judges and prosecutors) are not.

It also follows that LEAs (as of today) are not authorised (in accordance with the Italian DPA's decision on SARI-Real Time)[78] to install dynamic FR systems, while

[78] Decision n. 9575877, cit.

judicial authorities instead could possibly proceed to do so *proprio motu*, as they would not incur in a negative decision from the DPA. Further, according to art. 55 para 3 and recital 20 of the GDPR, national DPAs are not competent to judge on data processing operations undertaken by courts acting in their "judicial capacity", in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making.[79]

2.5.1. What will happen in the Municipalities after the moratorium? The cases of Udine and Lecce

It is difficult to predict what will happen in Municipalities when the moratorium expires (31 of December 2023) and until a European regulation that properly rules the use of FRTs will be approved.

What is undisputed is the strong will of local administrations to equip Local Police forces with these tools, as shown by the cases of Udine and Lecce.

As early as 2020, the Municipality of Udine had revealed interest in purchasing cameras equipped with FRT.[80] The announcement of the allocation of funds occurred before the intervention of the Italian DPA on the Como project. More recently, Mayor Pietro Fontanini expressed – at the "*Sicurezza Città di Udine 2023*" event – a strong disappointment with a warning received from the Italian DPA that prevented his Municipality from implementing of video surveillance cameras with

[79] The concept of "judicial capacity" was recently interpreted in a broad way by the ECJ in the *X and Z v Autoriteit Persoonsgegevens* judgment (Judgment of the Court, First Chamber, 24 March 2022, C-245/2020), "as not being limited to the processing of personal data carried out by courts in specific cases, but as referring, more broadly, **to all processing operations carried out by courts in the course of their judicial activity**, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority's competence".

[80] Anna Dazzan, "Udine, il comune stanzia 675mila euro per 67 videocamere a riconoscimento facciale. Ma non possono essere usate (per ora)", Il Fatto Quotidiano, 4 October 2021. Available here.

FR software.[81] In his statement, he stressed the importance of such a tool for crime prevention purposes and for the fight against terrorism, but he also demonstrated some confusion by equating FR with simple video surveillance, an error in which the Municipality of Como had already stumbled.

The Municipality of Lecce also announced in 2022 the launch of a system involving facial recognition technologies for urban security purposes. The Italian DPA, however, halted the project by opening an investigation on the mater and asking the Municipality to provide a description of the systems adopted, the purposes and legal basis of the processing and the data processing impact assessment, mandatory in the case of "large-scale systematic surveillance of an area accessible to the public." He then stressed that, during the moratorium, the use of FRTs is not allowed except for investigation by the judiciary or prevention and suppression of crimes.[82]

[81] The news is reported here.
[82] The document is available here.

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

The following section will analyse the approach of the Council of Europe's core institutions and bodies on the matter. The analysis will focus on the relevant rights protected by the European Convention on Human Rights ("ECHR") and the related interpretation of the European Court of Human Rights ("ECtHR" or "the Court of Strasbourg"). In light of the focus of this research, namely the use of FRTs by law enforcement and judicial authorities in the prevention and suppression of criminal offences. The research addresses Article 6 on the right to a fair trial, the principles embedded in the right (as interpreted by the ECtHR) as well as their application within the criminal justice systems. Particular attention will be placed on the implementation of these principles within the Italian context. The research will also address Article 8, which safeguards the right to privacy, and the requirements set out in Article 8 (2) which, if respected, qualify an infringement of the protected right as lawful. The analysis tries to assess whether the applicable Italian legislation on FRTs and the use of SARI-Enterprise comply with such criteria. The research also will look into Articles 10 and 11 safeguarding - respectively - the freedoms of expression and association, and the impact that FRT has on such fundamental freedoms.

Lastly, the analysis of the research will take into consideration other relevant (binding or soft law) instruments adopted by the CoE, including the so-called Convention 108+, the Guidelines of Facial Recognition Technologies and the so-called European Ethical Charter.

3.1 Article 6 ECHR

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private

life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proven guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights: (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; (b) to have adequate time and facilities for the preparation of his defence; (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

The right to fair trial, safeguarded in Article 6 ECHR, is a crucial milestone for democratic societies and an underlying principle to the rule of law pillar. While Article 6 covers the right to a fair trial in both civil and criminal proceedings, the focus of the following analysis will only concern criminal proceedings. It is worth highlighting that, as the Court of Strasbourg clarified, the guarantees contained in Article 6(3) for criminal proceedings are essential parts of the notion of the fair trial set out in Article 6(1).

On the use of FRT within criminal proceedings (meaning either used as a pre-investigative tool or as adduced evidence during the actual trial) **and their impact on the right to a fair trial under Article 6, there are no previous decisions of the ECtHR**. However, through its extensive case law, the ECtHR has developed core principles and criteria that can be applied to such issues as well. It is also worth mentioning that the analysed principles and safeguards are also part of the

Italian legislation and, therefore, are fully applicable to the use of FRTs by Italian law enforcement and judicial authorities, including while employing these tools within the framework of the moratorium.[83]

The crucial principle at the basis of Article 6 is the fairness of trials. What constitutes a fair trial depends on the circumstances of each case. According to the ECtHR, "compliance with the requirements of a fair trial must be examined in each case having regard to the development of the proceedings as a whole, and not based on an isolated consideration of one particular aspect or incident."[84] Nonetheless, the ECtHR states that in some circumstances, a specific element might be so decisive as to allow an assessment of the fairness of the trial even in an early stage of the procedure. Particularly, as part of that determination, "it needs to be assessed whether any measures taken in the previous stages weakened the applicant's position to such an extent that all subsequent stages of the proceedings were unfair."[85]

3.1.1. Article 6 (1)

The key principle of fairness contained in Article 6 applies to all criminal proceedings, regardless "of the type of offence at issue."[86] In determining whether the concerned proceeding has been fair as a whole, the ECtHR clarified that it is important to take into consideration "the weight of the public interest in the investigation and punishment of the particular offence has to be taken into consideration."[87] Nonetheless, concerns of public interest alone are not enough to

[83] See above para 2.4.
[84] European Court of Human Rights (ECtHR), *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)*, Updated on 31 August 2021, 7. Available here.
[85] Ibid.
[86] Ivi, 7.
[87] Ibid.

justify the failure to implement the essential elements of an applicant's due process rights.

- Equality of arms

Among the most relevant principles for the issue at stake, the principle of equality of arms is worth mentioning. Equality of arms is an "inherent feature of a fair trial."[88] According to the case law developed by the ECtHR, equality of arms requires that each party has a "reasonable opportunity to present the case under conditions that do not place them at a disadvantage *vis-à-vis* the opponent."[89] Another right that is traditionally considered closely related to the principle of equality of arms is the right to an adversarial hearing. The latter principle implies that the parties to a criminal proceeding must have the opportunity to be aware of and oppose every piece of evidence that has been filed by their counterparts and that consequently influence the decision of the court (such as the adduced evidence and observations). Due to the close connection between the two aforementioned principles, in some cases, the ECtHR found violations of Article 6 (1) by looking at the two principles together. Therefore, domestic legislation that fails to clearly express rules of criminal procedure may be in breach of the equality of arms principle as its main purpose is to safeguard the defendant against any abuse of authority. Therefore, the defence would be the most affected by lacunas and lack of clarity in such rules.

The equality of arms principle, however, might not necessarily be safeguarded when it comes to the use of FRT in the context of prevention and suppression of crimes, as in the Italian case at stake. For instance, while law enforcement and judicial authorities are well aware of the design and functioning of SARI-Enterprise

[88] Ivi, 34.
[89] Ibid.

(and of other FRTs tools which could be deployed in the future), as well as of the process followed by the system in order to obtain a specific outcome (i.e., a match in the AFIS-SSA database), the same cannot be said when it comes to the defence (or any other person affected by such use). This leads to an "imbalance" in the arms available, especially if the outcome of said FRT were to enter the trial as evidence, thus placing the defence at a disadvantageous position compared to the prosecutor. Moreover, this would create an additional burden on the defence when it comes to effectively challenging (and opposing) the use of a piece of evidence - an element that is assessed as fundamental by the Court of Strasbourg to consider the trial as a whole as fair.[90]

- Admissibility of evidence

While Article 6 lays down the right to a fair trial, it does not explicitly governs the admissibility of evidence as such, which remains mostly a matter regulated by domestic legislation.[91] As clarified by the ECtHR, "it is not [...] the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible."[92] Consequently, the Court of Strasbourg would ("only") assess whether the proceedings as a whole were fair, including how the evidence was acquired (the so-called overall fairness test). This involves an examination of the alleged unlawfulness and the nature of this violation when the breach of another

[90] See the arguments analysed on the para. below on the "Admissibility of evidence".

[91] See, among others, European Court of Human Rights, *Schenk v. Switzerland*, Application No. 10862/84, 12 July 1988, § 46 (available here); and *Garcia Ruiz v. Spain*, Application No. 30544/96, 21 January 1999, "while Article 6 of the Convention guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence or the way it should be assessed, which are therefore primarily matters for regulation by national law and the national courts" (§ 28) (available here).
For the matter at stake, see above the Italian context and relevant legislation at para 2.1.

[92] European Court of Human Rights (ECtHR), *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb), cit.*, 44.

right protected by the Convention is concerned. According to the ECtHR case-law, the sole fact that a piece of evidence has been unlawfully obtained would not lead to consider the proceedings as unfair.[93] The overall fairness test would apply in cases regarding whether the use of information allegedly obtained in violation of Article 8, and submitted as evidence into a trial, renders the whole trial unfair under Article 6. In such circumstances, the Court of Strasbourg would consider if the unlawful acquisition of evidence impacts the reliability of the evidence itself (although quite rare). In addition, the ECtHR would pay attention at the circumstances in which the evidence was obtained, including "whether these circumstances cast doubt on its reliability or accuracy,"[94] as well as the quality of such evidence. However, it can be pointed out that this results to be "problematic in cases where evidence is obtained in violation of Article 8, because the reliability of such evidence – recordings, intercepted correspondence or other evidence obtained without a warrant – is rarely in doubt."[95] In cases concerning the use of evidence obtained by (unlawful) secret surveillance - as in *Bykov v. Russia,*[96] *Khan*

[93] The ECtHR, however, excluded evidence the use of which violated the integrity of the trial and the rule of law. It indeed considered the trial as unfair in cases in which the evidence has been obtained in violation of absolute rights protected by the Convention, such as the prohibition of torture and other inhuman and degrading treatment (Article 3 ECHR - see European Court of Human Rights, *Gäfgen v. Germany,* Application No. 22978/05, 1 June 2010, §§ 98-99 - available here); or in violation of some relative rights, when the use of such evidence would amount to a "flagrant denial of justice". For example, when there has been entrapment or incitement from the law enforcement authorities and there has been no other indication that the offence would have been committed anyway (see European Court of Human Rights, *Teixeira de Castro v Portugal,* Application No. 25829/94, 9 June 1998, §§ 38-39 - available here); or when there have been serious violation of the right to cross-examination (see European Court of Human Rights, *Vidgen v the Netherlands,* Application No. 29353/06, 10 July 2012 - available here). Ligeti K., Garamvölgyi B.,Ondrejová A., and von Galen M., *Admissibility of Evidence in Criminal Proceedings in the EU, The Future of EU Criminal Justice - Views from the Experts*, eucrim 3/2020, 205. Available here.

[94] European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)*, *cit*. 44.

[95] Fair Trials, *Unlawful evidence in Europe's courts: principles, practice and remedies*, October 2021, 21. Available here.

[96] [GC] 2009 §§ 69-83.

v. the United Kingdom,[97] *Dragojević v. Croatia,*[98] *Dragoş Ioan Rusu v. Romania,*[99] *Falzarano v. Italy,*[100] *Lysyuk v. Ukraine*[101] - the ECtHR never found a violation of Article 6, considering, therefore, the trial fair overall, despite the fact that it found a violation of Article 8, as one or more of the requirements outlined in Article 8 (2) had not been satisfied.[102]

In the determination of whether the proceeding as a whole was fair, the rights of the defence and if such rights have been complied with, need to be taken into consideration.[103] This implies that the ECtHR would evaluate whether the defence could **effectively** challenge the use of the concerned evidence unlawfully obtained.[104] In the *Dragoş Ioan Rusu v. Romania* case, which concerned an unauthorised interception of correspondence of the applicant for a drug investigation, the ECtHR found that the procedure for authorisation did not afford sufficient safeguards in accordance with Article 8 (2) ECHR. Nonetheless, the ECtHR also noted that the applicant challenged the (un-)lawfulness of the surveillance in the criminal proceedings and that the reliability of such evidence

[97] 2000 § 34.
[98] 2015 §§ 127-135.
[99] 2017 §§ 47-50.
[100] 2021 §§ 43-48.
[101] 2021 §§ 67- 76.
[102] See, as a way of example, European Court of Human Rights, *Schenk v. Switzerland,* Application No. 10862/84, 12 July 1988 (recording telephone conversation); *Khan v. United Kingdom*, Application No. 35394/97, 12 May 2000 (covert listening device) - available here; *Perry v. United Kingdom*, Application No. 63737/00, 26 September 2002 (video surveillance) - available here; and *Lee Davies v. Belgium*, Application No. 18704/05, 28 July 2009 (illegal search) - available here- quoted by McBride J., *Application of the European Convention on Human Rights and harmonisation of national legislation and judicial practice in line with European standards in Georgia*, European Union - Council of Europe joint project, footnote 102. Available here.
[103] European Court of Human Rights (ECtHR), *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)*, *cit,* 35-37.
[104] Fair Trials, *cit*., 16.

was not questioned, and for this reason, the ECtHR did not consider the trial to be unfair.[105]

The ECtHR's argument regarding the possibility of the defendant challenging evidence brings back the above-mentioned remarks concerning the employment of FRT in the criminal justice system and the existing imbalance of arms between the prosecution and the defence. An additional argument which could be made is linked to the financial situation of the concerned defendant in relation to the possibility of hiring an external consultant as an expert witness to challenge the output of an FRT. Indeed, besides the limited number of experts available in Italy who would have the expertise to (re-)carry out the algorithmic process that led to the outcome adduced as evidence, hiring an expert witness is expensive. This would not only lead to another element of imbalance of arms but also to an indirect (financial) discrimination of the defendant. Such a discriminatory practice would not be tolerated within the criminal justice system: for instance, the principle of non discrimination, as expressed by the so-called European Ethical Charter,[106] is at the core of the notion of "fair trial", and it implicitly requires the proceedings not to be discriminatory against any party. Therefore, such discrimination would - substantially - result to be also contrary to the values of a democratic society.

Let us assume now that a defendant has the financial capacity to sustain the cost of hiring an external consultant who is able to clearly explain the procedure (theoretically) applied by a FRT to obtain such an outcome. Even so, it would be almost impossible for the consultant to reproduce the very *same* procedure conducted by the system in the first place, due to the obscurity in its functioning mentioned above. This would be necessary in order to demonstrate that the

[105] European Court of Human Rights, ***Dragoş Ioan Rusu v. Romania***, Application No. 22767/08, 31 October 2017, §§ 36-44. Available here.
[106] See below para 3.4.

concerned outcome was incorrect due to several reasons, including the biassed database used by the algorithm and would represent yet another obstacle to the required equality of arms in the criminal trial.

3.1.2. Article 6 (2)

Article 6 (2) recognises and safeguards the presumption of innocence. This principle, in the criminal sphere, requires *inter alia* that the members of the concerned court (either national or international/supranational), in performing their duties, should not have from the beginning the biassed idea that the accused person has committed the charged offence; and that the burden of proof falls on the prosecution. The presumption of innocence requires numerous conditions in respect of the premature expressions, by the trial court or by other public officials, of a defendant's guilt and the burden of proof - as mentioned; as well as of legal presumptions of fact and law; pre-trial publicity; and the privilege against self-incrimination. The presumption of innocence is considered an essential procedural guarantee in the context of a criminal trial itself.

When analysing the possibility of using AI-related evidence (as those gathered through FRTs) in the criminal justice system, one should mention the concept of "automation bias". Automation bias involves "the tendency to over-rely on automation in ways that can cause errors in decision making."[107] It entails that a person is bound to consider technology as more reliable and trustworthy in comparison to a human-made decision. However, the outcomes provided by the AI machine are based on algorithms, which require an initial set of data or information to be able to produce results. This implies that automated outcomes can be unreliable when the data inserted as starting point is incorrect, inaccurate, or "pre-biased". In other words, "[t]he way in which AI [...] systems are designed,

[107] Fair Trial, *Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU*, 2022, 25. Available here.

created, and operated can lead to biassed and ultimately discriminatory outcomes."[108] In addition,

> [t]he type of AI [...] designed or created for use in the criminal justice system will almost inevitably use data which is heavily reliant on or entirely made up of law enforcement data, crime records or other criminal justice authorities' data. These data and records do not represent an accurate record of criminality, but merely a record of law enforcement, prosecutorial or judicial decisions – the crimes, locations and groups that are policed, prosecuted and criminalised within that society, rather than the actual occurrence of crime.[109]

While these tools are now used throughout Europe in implementing the so-called preventive or proactive policing (as opposed to the traditional reactive policing) of law enforcement and other judicial authorities, automated decisions might highly impact (and undermine) the presumption of innocence. Indeed, "people cannot and should not be preemptively judged as guilty"[110] until his/her guilt is fully proven through corroborating pieces of evidence.

Among those principles implied in the presumption of innocence, the one concerning the burden of proof is also worth clarifying. The principle implies that the prosecution shall inform the accused person of the charges made against him/her/them and submit related evidence, so that the charged person may be prepared and file the defence accordingly. Consequently, the presumption of innocence is violated every time the burden of proof (wrongfully) lies on the defence, rather than on the prosecution. In the case at stake, it could be argued that the use of FRTs, such as the SARI-Enterprises and SARI-Real Time, could

[108] Ivi, 27.
[109] Ibid.
[110] Ivi, 30.

represent an **unlawful and unjustified reversal of the burden of proof from the prosecution to the defence**. For instance, the defence would be practically asked to question the reliability of the evidence without having at its disposal any information on the design and the functioning of the FRT, making it impossible to effectively grasp the procedure followed by the system to obtain the outcome used as evidence. As mentioned above, this would also represent a disbalance in the "arms" at the disposal of the two parties (prosecutor and defence) as well as an obstacle in effectively challenging the admissibility of the concerned evidence. Moreover, the employment of FRT would affect the presumption of innocence of the concerned defendant, as s/he would be the one demonstrating to the judge that s/he is not guilty of the charged offence, rather than the prosecution proving his/her guilt and the judge would start the proceedings already with a sort of bias.

3.1.3. Article 6 (3)

As previously mentioned, the requirements laid down in Article 6 (3), which governs the rights of the defence, need to be considered as an essential part of the right to a fair trial. For instance, the aim of the specific guarantees explicitly mentioned in Article 6 (3) is "always to ensure, or to contribute to ensuring, the fairness of the criminal proceedings as a whole."[111] Therefore, the guarantees enshrined in Article 6 (3) must be interpreted accordingly, namely in the light of their "function" within the overall proceeding. The rights which are part of the more general "right of defence" have been established and safeguarded by the Convention (through the non-exhaustive list of Article 6 (3) (b)), whose main aim is establishing equality between the parties, namely the prosecution and the defence).[112]

[111] European Court of Human Rights (ECtHR), *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)*, cit, 76.
[112] European Court of Human Rights (ECtHR), *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)*, cit, 80.

- Conclusions

Despite the absence of specific ECtHR case law on the matter at stake, the CoE as well as academics have laid out the risks the use of FRTs, and AI more generally, has on the right to a fair trial. For instance, as stated by the research carried out in 2021 by The Alan Turing Institute, and published by the CoE, "AI can adversely affect the liberty and justice of individuals, particularly when implemented in high impact contexts such as criminal justice. The complexity and opacity of AI systems may interfere with the right to a fair trial including the right to equality of arms [...]. judicial decisions supported or informed by AI may negatively affect the rulemaking and decisional independence of the judiciary."[113]

Similarly, it was highlighted that when it comes to analysing the compatibility between AI and the traditional purposes and safeguards of the criminal trial, together with the evidentiary process, AI can affect the principles of the presumption of innocence, equality of arms and adversarial process, among others.[114]

These are some of the risks of abuse that would arise from the employment of Italian FRTs, such as SARI, to the due process and fair trial guarantees at the European level, which needs to be complied with by Italy as well. This would raise doubts about every decision taken by Italian judicial authorities through the deployment of FR tools. No judgement has been found as regards the employment of AI tools (including FRT) to justify pre-trial detention measures and the related approach of the Court of Strasbourg on this matter.

[113] Council of Europe's Ad Hoc Committee on Artificial Intelligence and The Alan Turing Institute, "*Artificial Intelligence, Human Rights, Democracy, and the Rule of Law*", 2021, 16. Available here.
[114] Eftychia Bampasika, *Artificial Intelligence as Evidence in Criminal Trial*, 2020, 2. Available here.

3.2 Article 8 ECHR

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

When it comes to assessing whether FRTs affect any fundamental right, it is straightforward thinking about the (potential) intrusion of such tools within individuals' privacy. Despite the limited provision within the ECHR, through its extensive case law, the Court of Strasbourg has been able to include within the safeguard of Article 8 the individuals' and collective right to privacy (i.e. the latter intended as referring to mass surveillance) as well as data protection.[115] This is how the ECtHR can assess whether cases of mass surveillance, the use of artificial intelligence and/or FRT are in breach of Article 8.

The provision of, and thus the rights protected in, Article 8 is not absolute; and exemptions to the rights enshrined in Article 8 (1) are allowed. However, the criteria listed in Article 8 (2) need to be met. Through its extensive case law, and based on the provision of Article 8 (2), the ECtHR has indeed developed a sort of test that is applied to any single time it has to assess whether there has been an unlawful interference with the provision of Article 8 (1). For instance, Article 8 (2) requires that the inference conducted by the public authority shall take place "in accordance with the law"; that it shall pursue one of the mentioned aims listed, such as national security, and the prevention of disorder or crime - among others; and, lastly, that it

[115] Council of Europe, *Privacy and data protection*. Available here.

shall be a measure "necessary in a democratic society", i.e., a proportionate interference compared with the pursued aim.

Furthermore, according to the ECtHR, in balancing two different interests, namely to safeguard national security through surveillance measures, including FRTs, and to avoid serious interferences to individuals' right to privacy, domestic authorities hold a margin of discretion. In its decisions, the ECtHR has clarified how such requirements need to be satisfied for the interference to be considered lawful (the so-called three-part test):

1. **"[l]In accordance with the law"** means that the contested provision needs to have a legal basis in the domestic law. Not only: it also involves considerations related to the quality of the law, meaning its accessibility to the concerned person (i.e. it needs to be accessible and precise); as well as its foreseeability. Therefore, the domestic law shall adopt a transparent legal framework able to provide for the indication of the situations under which public authorities have the power, and the legitimacy to use such technologies.[116]

   The CJEU has recently addressed a similar issue, namely the compatibility of an EU country's national legislation allowing the processing of biometric data with the relevant EU provisions (specifically, the GDPR and the LED). In analysing the requirement "provided by law", the CJEU reiterated that such criterion should be interpreted as implying that the concerned legal basis allowing an interference with the protected rights shall define in a clear and precise way the scope of such limitation.[117]

[116] See, among others, European Court of Human Rights, *Roman Zakharov v. Russia*, Application No. 47143/06,4 December 2015 - available here; and European Court of Human Rights, *Kennedy v. United Kingdom*, Application No. 26839/05, 18 May 2010 - available here.
[117] For further analysis, see below at para 4.7.

For instance, the use of SARI Real-Time by law enforcement and judicial authorities (as well as by other public authorities, such as municipalities - should the moratorium not be renewed by the end of 2023) was already considered by the Italian DPA[118] as **lacking sufficient legal basis**, hence in violation of Article 7 of Legislative Decree 18 May 2018, n. 51.[119] Article 7 leg. Decree 51/2018 explicitly requires that the processing of data mentioned in Article 9 of the GDPR, including biometric data, must be authorised only if strictly necessary, and suitable safeguards exist for the rights and freedoms of the data subject, and are specifically provided by the EU law or the domestic law. While the Italian Government has presented several provisions of the Code of Criminal Procedure as "possible" legal basis for the use of SARI Real Time, the Italian DPA did not consider them sufficient to satisfy the requirement of a **suitable legal basis for the processing of biometric data aimed at personal identification via SARI-Real Time**. A similar conclusion - which identifies a violation of Article 8 (2) ECHR - could be adopted by the Court of Strasbourg should public authorities continue deploying SARI "for the prevention and suppression of crimes" and the Italian legal framework remains the same.

2. It shall **pursue one of the legitimate aims** referred to in Article 8 (2), namely the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

3. "**[N]ecessary in a democratic society**" (the so-called necessity and proportionality test) implies that inferences with the rights of Article 8 (1) are lawful only to pursue one of the legitimate aims listed in the provision (and

[118] See decision of 25 March 2021, cit.
[119] See para. 2.2.1. above.

above), without affecting the "objective and purpose" of the protected rights. Thus, the ECtHR demanded State Parties adopt **adequate and effective guarantees against abuse**. In the landmark *Weber and Saravia v. Germany* case (2006), the ECtHR elaborated the so-called *six Weber criteria* necessary to avoid abuse of power and arbitrariness from public authorities and national intelligence services during interferences with the right to privacy.[120] Such criteria, which should be established in national legislative norms regarding espionage, are recalled in each subsequent judgement of the ECtHR, still influencing the Judges' work. In particular, the Court of Strasbourg requires, firstly, "the nature of the offences which may give rise to an interception order"; then "a definition of the categories of people liable to have their telephones tapped" and "a limit on the duration of telephone tapping"; fourth "the procedure to be followed for examining, using and storing the data obtained"; then, "the precautions to be taken when communicating the data to other parties"; and, finally, "the circumstances in which recordings may or must be erased or the tapes destroyed"[121] have to be defined by the domestic legislations. The ratio of the establishment of such criteria is noticeable considering that surveillance activities involve the risks of potentially being able to undermine or even destroy a democratic system rather than safeguarding it.[122] Concluding, domestic law shall provide for adequate and effective safeguards against arbitrary and unlawful interference, precisely against its abuse. To comply

[120] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer, *Mass Surveillance on Personal Data by EU Member States and its Compatibility with EU Law*, CEPS Paper in Liberty and Security in Europe, N. 62, 2013, 15. Available here.

[121] European Court of Human Rights, Application. No. 54934/00, *Weber and Saravia v. Germany*, 29 June 2006, § 95. Available here.

[122] European Court of Human Rights, Research Division, *Internet: case-law of the European Court of Human Rights*, 2015.

with these recommendations, the ECtHR will take into consideration "all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."[123]

Since the ECtHR often recognised the margin of discretion enjoyed by national authorities in determining the measures considered adequate to protect national security, in its case-law (precisely, in the mentioned *Weber and Saravia* case and the *Liberty and others v. UK* case), it even accepted that mass surveillance did not per se go beyond this margin. In fact, due to the developments of technologies – also used by terrorists and criminals to circumvent a more "targeted" control – combined with the global threats of terrorism and serious crimes (such as cybercrime), the Judges noted that precisely the decision to implement a bulk surveillance regime to fight against these threats falls within the idea of margin of appreciation.

Notwithstanding these considerations, as from the ECtHR case law emerges, every type of espionage regime can potentially be abused, thus the Court of Strasbourg called upon State Parties to implement the minimum safeguards – the six Weber criteria – concerning both targeted and bulk surveillance to reduce the risks of abuse of power.[124] Moreover, while analysing this requirement, the ECtHR assesses whether the measure is proportionate to the legitimate aim and whether the same purpose cannot be achieved by a less restrictive method. In *LL v. France*, the ECtHR made clear that "[i]n order to ascertain whether the impugned

[123] European Court of Human Rights, *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application. No. 62540/00, 2007, § 77. Available here.
[124] European Court of Human Rights, *Centrum för Rättvisav, Sweden*, Application. No. 35252/08, 19 June 2018. Available here.

> measure was "necessary in a democratic society", [it] will consider, **in the light of the case as a whole and having regard to the margin of appreciation enjoyed by the State in such matters**, whether the reasons adduced to justify it were relevant and sufficient and whether the measure was proportionate to the legitimate aim pursued."[125] Similarly, in *S. and Marper v. UK*, the ECtHR's Grand Chamber pointed out that "[t]he question is [...] whether [the contested measure] is proportionate and strikes a fair balance between the competing public and private interests."[126] In addition to the scope, the domestic law should also express the duration of the surveillance measure carried out.[127] Furthermore, usually, to limit domestic authorities' discretion in interpreting the scope of surveillance measures, the ECtHR also requires prior authorisation to the use of such technology: "interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[128] The ECtHR also requires an *ex-post* control conducted by a national judicial oversight.

It is worth mentioning the extensive case law addressed by the ECtHR throughout the years on the topic of targeted secret surveillance (which is opposed to the so-called bulk or mass surveillance which characterised the use of FRTs or AI more

[125] European Court of Human Rights, *LL v. France*, Application no. 7508/02, 10 December 2006, para 43. Available here.
[126] European Court of Human Rights, *S. and Marper v. United Kingdom*, Applications Nos. 30562/04 and 30566/04, 4 December 2008, § 118. Available here.
[127] See, *inter alia*, European Court of Human Rights, *Kennedy v. United Kingdom*, Application No. 26839/05, 18 May 2010 - Available here; and European Court of Human Rights, *Uzun v. Germany*, Application No. 35623/05, 2 September 2010 - Available here.
[128] European Court of Human Rights, *Centrum för Rättvisa v. Sweden*, Application No. 35252/08, 19 June 2018. Available here.

generally), starting from the well-known *Klass and Others v. Germany* (1978) *Weber and Saravia v. Germany* case (2006); *Liberty and Others v. The United Kingdom* (2008), and *Szabò and Vissy v. Hungary* (2016), among others.

With the verdict in *Roman Zakharov v. Russia*,[129] the ECtHR eventually began to evaluate the mass surveillance system's compliance with the Convention in 2015. The ECtHR analysed whether not only the stage of collection of data, but also its storage, processing, and use are compatible with Article 8 (2) ECHR. The latest decisions issued by the ECtHR's Grand Chamber have been *Centrum för Rättvisa v. Sweden* (2021);[130] and *Big Brother Watch and others v. the UK* (2021).[131]

Unfortunately, in both cases - even if the ECtHR found violations of Article 8 for the specific circumstances at stake - it held that mass surveillance systems are not per se incompatible with the principles of the Convention. However, "such a regime must be subject to certain "end-to-end safeguards", meaning that, at the domestic level, an assessment of proportionality should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review."[132]

Concerning the use of FRTs, only a few cases have been addressed by the ECtHR. According to the ECtHR, however, the accelerated development - in the last years - of sophisticated technologies, such as FRTs and facial mapping tools

[129] European Court of Human Rights, *Roman Zakharov v. The Russian Federation*, cit.
[130] Available here.
[131] Available here. For a detailed explanation, see here, Lo StraLe, *La Vittoria di Pirro del Diritto alla Privacy*, 21 September 2021 (ITA).
[132] European Court of Human Rights, *UK surveillance regime: some aspects contrary to the Convention*, Press Release issued by the Registrar of the Court, ECHR 165 (2021), 25 May 2021, 1. Available here. See also Blackstone Chamber, *Big Brother Watch and Others v the United Kingdom*, 26 May 2021. Available here.

applicable to individuals' photographs, "makes the taking of their photographs and the storage and possible dissemination of the resulting data problematic."[133] The Court of Strasbourg also pointed out that while assessing the necessity of interference with the rights protected in Article 8 (amongst others, the private life of individuals), domestic courts shall also take into account these factors and developments.[134]

One of the latest cases analysed by the ECtHR is *Guaghran v. the UK* (2020).[135] In this case, it stated that the employment of FR tools, namely the use of photos acquired during a person's arrest and then stored in a police database represented an unlawful interference with the right to private life under Article 8. The ECtHR also pointed out that retaining photos of arrested persons for an indefinite period of time represents a violation of the same right under Article 8.[136] However, it is worth highlighting that:

1. The ECtHR clearly stated that "**the concept of private life included elements relating to a person's right to their image**" (§66);

2. The focus of the whole judgement has not been the capture or the use of the image of the victim as evidence for his conviction in the criminal proceeding, rather the regime of indefinite retention of such images which was considered in violation of Article 8 ECHR ("[...] in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the ECtHR will have due regard to the specific context in which the information at issue has been recorded and

[133] European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights, Data protection*, updated on 31 August 2021, 86. Available here.
[134] Ivi.
[135] European Court of Human Rights, *Gaughran v. the UK*, cit.
[136] Manon Laganà, *Facial Recognition And Human Rights In Europe*, Human Rights Pulse, 1 April 2022. Available here.

retained, the nature of the records, how these records are used and processed and the results that may be obtained", §66; and "[...] the retention at issue constitutes a disproportionate interference with the applicant's right to respect for private life and cannot be regarded as necessary in a democratic society", §97);

3. The ECtHR has accepted that the use of biometric surveillance technologies as well as the retention of such data does not - in principle - violate Article 8 ECHR: "retention of biometric data and photographs pursues the legitimate purpose of the detection and, therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the particular crime of which they are suspected, its retention pursues the broader purpose of assisting in the identification of persons who may offend in the future", §75.

This has been the result of a previous case-law in which the Court of Strasbourg reiterated the same principles (see, as a way of example, *S. and Marper v. the UK;*[137] or *Beghal v. the UK,*[138] where the ECtHR referred to using FRT in airports or ports by immigration or anti-terrorism officers, concluding that such practices were consistent with Article 8 (2) ECHR since said measures were used just for public security and national defence purposes, being therefore compliant with the law of the country.).

It is worth mentioning the legal framework as well as the practice related to the **retention of data in the Italian system**. Data and information obtained through FRTs, among others, for prevention and suppression of criminal offences'

[137] European Court of Human Rights, *S. and Marper v. the UK*, Applications Nos. 30562/04 and 30566/04, 4 December 2008. Available here.
[138] European Court of Human Rights, *Beghal v. the UK*, Application No. 4755/16, 25 May 2019. Available here.

purposes, converge into a database called C.E.D. (*Centro di elaborazione dati*). The C.E.D. was established within the Department of Public Security of the Ministry of the Interior by Article 8 of Law 121/1981.[139] Explicitly, Law 121/1981 affirms that law enforcement authorities are required to promptly report to the C.E.D. information acquired during activities of investigation (Article 7 (1)). The Italian legislation theoretically aims at safeguarding the right to privacy of individuals through the Legislative Decree 196/2003 (which was implemented in the Italian system as Directive 95/46/EC,[140] currently replaced by the GDPR)[141], which (allegedly) ensures "the periodic updating and the relevance and non-excessiveness of the personal data processed, including through authorised queries of the criminal records and the pending charges records of the Ministry of Justice"[142] (Article 54 (3), Title II); as well as through the Decree of the President of the Italian Republic 5/18, which implements the principles on privacy protection to the data retained in the C.E.D. This Decree states that the retention of data is allowed for "a period of time not exceeding that necessary for the achievement of police purposes". Particularly, Article 10 lists the period of retention of data which varies from 3 to 30 years, for different criminal offences. The problems arise when it comes to the actual update of the C.E.D.: the legislation requires the automatic update of the database, based on the outcomes of criminal investigations or proceedings. In practice, this does not happen, and therefore the concerned person needs to file a special request to update or delete the records from the

[139] Law 1 April 1981, n. 121, Published in the Official Journal (*Gazzetta Ufficiale*) on 10 April 1981, n. 100, New order of the Public Security Administration. Available here.
[140] 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 of such data - no longer in force. Available here.
[141] See below para. 4.7.
[142] From the Italian version *"l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati anche attraverso interrogazioni autorizzate del casellario giudiziale e del casellario dei carichi pendenti del Ministero della giustizia".*

database.[143] This implies **an excessive burden to the concerned person**, who should present a request through a lawyer and justify the special reason(s) for which s/he requires the updating or deletion of such data.

As the period of retention of data in a police database is concerned, as the ECtHR already in 2010 (case *Brunet v. France*) explicitly stated, the respect for the requirements set out in Article 8 (2) ECHR is even more necessary when it comes to the protection of personal data subject to automatic processing, in particular when such data are used for police purposes. Domestic law shall ensure that such data are relevant and proportionate to the purposes pursued through the retention and that such retention does not exceed the necessary period of time. Domestic law shall also provide for safeguards to ensure that retained personal data are effectively protected against misuse and abuse.[144] While specific periods of time are clearly mentioned in the Italian legislation, little explanations are provided when it comes to the necessity and proportionality of data retained for 20 years or more. Therefore - using the words of the Court of Strasbourg - **Italian law**, as of today, would represent a **disproportionate interference with individuals' right to respect for private life** and cannot be considered necessary in a democratic society. In the aforementioned 2010 judgement, the ECtHR continued stating that, in assessing the proportionality of the length of time for which information is stored in the light of the purpose for which it was gathered, it takes into account whether or not there is an independent review of the justification for its storage in the processing system, based on specific criteria such as the seriousness of the offence, previous arrests, the strength of the suspicions against the person or any other special circumstances.[145] It is worth noting that such independent review,

[143] Consulenza Legale Italia, *Precedenti di polizia e la cancellazione dal C.E.D – una guida rapida*. Available here.
[144] European Court of Human Rights, *Brunet v. France*, Application No. 21010/10, 18 September 2014 §35. Available here (French only).
[145] Ivi, §36.

which should regularly verify if the justification for the retention still exists but is *not* present in the Italian context. Lastly, the Court of Strasbourg (2010) paid particular attention to the risk of "stigmatising" individuals who, as the person in the concerned judgement, have not been convicted of any crime and are entitled to be presumed innocent[146]. As shown above, within the context of C.E.D., retained data are not deleted or updated automatically, neither after the conclusion of the relevant investigation or police activities nor after the completion of the period of time expressed by the concerned provision. These circumstances represent both a violation of Article 8 as well as of Article 6 ECHR.

- Conclusions

From the above stems that to understand whether the current Italian legislation[147] complies and is in line with the standards set out by Article 8 and the related ECtHR case-law, it would need to undergo a detailed assessment from the Court of Strasbourg. It is worth stressing again that the requirements of Article 8 (2) as interpreted by the ECtHR would need to be present in an even stricter sense within the criminal justice system, due to the impact that criminal trials have on individuals' fundamental rights (such as the right to liberty).

3.3 Articles 10 and 11 ECHR, including in combination with Article 14 ECHR

Article 10 ECHR:
"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by

[146] Ivi, §38.
[147] See also above paras. 2.1 onwards.

public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Article 11 ECHR:

1. *Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.*

2. *No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.*

Article 10 and Article 11 of the ECHR recognise and protect two crucial rights, namely freedom of expression, and freedom of assembly and association. Both freedoms are not absolute, and - therefore - exemptions are allowed when specific criteria are met.

There is no available ECtHR's case-law on the matter at stake (neither taking Articles 10 or 11 ECHR alone nor in combination with Article 14 ECHR),

however, the use of FRTs will affect the enjoyment of these two rights by having a chilling effect on the society.

This has been confirmed by the CoE, in a study published in 2021 and conducted by The Alan Turing Institute: the unregulated use of FR, and AI more generally, can highly affect the enjoyment of such rights. For instance, "[l]ive facial recognition systems may prevent citizens from exercising their freedoms of assembly and association, robbing them of the protection of anonymity and *having a chilling effect on social solidarity and democratic participation.*"[148]

3.4 Council of Europe instruments

In 1981 the Council of Europe adopted the first legally binding instrument in the data protection area,[149] namely the so-called **Convention 108** (or 1981 Convention, *i.e.* the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).[150] As such, the Convention provides relevant definitions for the analysis of the matter at stake, namely the employment of FRT by law enforcement and judicial authorities during criminal investigations and following trials. For instance, Article 2 clearly defines "personal data" as any information able to identify the so-called data subject (i.e. "*an identified or identifiable individual*") (a); and "data processing" as "*any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or*

[148] Council of Europe's Ad Hoc Committee on Artificial Intelligence and The Alan Turing Institute, "*Artificial Intelligence, Human Rights, Democracy, and the Rule of Law*", 2021, 16.
[149] Bruno Saetta, *Convenzione 108 del Consiglio d'Europa*, Protezione dati personali/Data Protection, 2018. Available here.
[150] In 2018, the *Ad hoc* Committee on Data Protection issued the so-called Convention 108+ (i.e. the Protocol amending the 1981 Convention). The Convention has been adopted during the 128th session of the Committee of Ministers of May 2018. The purpose of the Amendment was to modernise the Convention 108 in line with the increased development of new technologies. Available here.

destruction of, or the carrying out of logical and/or arithmetical operations on such data" (b).[151] Article 5, headed "Legitimacy of data processing and quality of data" recalled the principles and criteria of Article 8 (2) ECHR, namely the fact that **personal data undergoing automatic processing has to be obtained fairly, in a proportional way according to the specific purposes** and, consequently, that data cannot be used in incompatible methods for these purposes. This is particularly important to the issue of deploying FR technologies, as it implies the necessity and proportionality of the measure taken vis-a-vis the affected right(s). The Convention continues by pointing out that personal data cannot be stored for longer than necessary; it is prohibited to process sensitive data, such as race, political opinions, and health, including genetic data and biometric ones, without adequate guarantees enshrined by the law. Data security in each process also needs to be granted to avoid risks of accidental loss, unauthorised access or alteration of personal information. Article 10 (3) requires each State Party to make sure that "*controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing*".

Article 11 allows **exemptions** to the mentioned provisions and safeguards only when it is necessary to protect public interests (including the **prevention, investigation and prosecution of criminal offences and the execution of criminal penalties**), data subjects or rights and liberties of other individuals. However, as in Article 8 (2) ECHR, the exception needs to be "*provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society*". Such criteria would

[151] Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 128th Session of the Committee of Ministers, 2018, Article 2, lit. *b*.

need to be interpreted according to the meaning provided by the ECtHR.[152]

Chapter IV governs the "Supervisory authorities" tasked to ensure the "compliance with the provisions of this Convention" (Article 15). To this aim, the instrument provides to them some functions, including the power of investigation and intervention, to bring the attention of the competent judicial authority and to hear claims of individuals regarding their rights involving the treatment of personal data as well as to impose administrative sanctions. In 1996, Italy established the DPA (*Garante per la Protezione dei Dati Personali*) when implementing the EU Directive 95/46[153] (currently replaced by the so-called GDPR). Italy also ratified Convention 108+, including the mentioned Article 15, and was published in the Official Journal (*Gazzetta Ufficiale*) in May 2021.[154] Nonetheless, despite the similar functions and powers, Italy has not based the legislation establishing the DPA on the concerned provision - leading therefore to a possible breach of its CoE's obligations.

According to Article 4 (1), each State Party to the Convention must "take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application". As Italy has ratified the 1981 Convention in March 1997 and entered into force in July 1997,[155] this implies that such provisions and obligations fully bind the Italian institutions and bodies, including the law enforcement and judicial authorities while operating in the context of prevention and suppression of criminal offences through FRT. For the analysis at stake concerning the employment of FRT by law enforcement and judicial authorities

[152] See above para 4.2.
[153] 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 of such data - no longer in force. Available here.
[154] Gazzetta Ufficiale, Legge 22 aprile 2021, n. 60. Ratifica ed esecuzione del Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018. (21G00068) (GU Serie Generale n.110 del 10-05-2021). Available here.
[155] See Parties to the Convention 108, here.

within criminal proceedings, it is important to mention the "*Guidelines on Facial Recognition*" adopted in 2021 by the CoE to provide a set of references that governments and public authorities, FR developers, and service providers should follow and apply to ensure that FRT does not disproportionately affect human rights and fundamental freedoms of anyone.[156] When it comes to the employment of FRT by public authorities, the Guidelines clarified that the "*[b]iometric data processing by facial recognition technologies for identification purposes in a controlled or uncontrolled environment should be restricted, in general, to law enforcement purposes. It should be carried out solely by the competent authorities in the area of security.*"[157] While requiring the respect of the principles of necessity and proportionality according to Convention 108+ (as well as to ECHR), the Guidelines allow domestic law to provide for different necessity and proportionality tests based on the purpose for which the FRT has been used by law enforcement authorities, namely verification or identification. Particularly, "[f]or **identification purposes**, the **strict necessity and proportionality must be observed both in the setting-up of the database (watchlist) and deployment of (live) facial recognition technologies.**"[158] Domestic law needs to provide accurate criteria for law enforcement authorities to comply with when designing databases (watchlist) "for specific, legitimate and explicit law enforcement purposes (for example suspicion of severe offences or risk to public security)."[159] When it comes to the employment of live FRT (like SARI- Real Time in the Italian context), national law has to ensure that law enforcement authorities can prove that several factors, such as the time and place of deployment of such technologies, comply with the strict necessity and

[156] The *Guidelines on Facial Recognition* adopted in January 2021 by the Committee of Convention 108 are available here.
[157] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108, *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 January 2021, 6.
[158] Ibid.
[159] Ibid.

proportionality test. Lastly, while the obligation of transparency (as per Article 8 of the Convention 108+) is binding both public and private sectors to provide detailed information about the processing, the Guidelines pointed out that the transparency obligation may be proportionately limited in cases where databases are created by law enforcement authorities for identification or verification reasons so as not to interfere with their efforts. For instance, law enforcement authorities can use a layered strategy to provide the relevant information to data subjects transiting through the uncontrolled environment when live FRT is deployed there. LEAs may only clandestinely utilise live FRT if it is absolutely required and proportional to stop a serious and immediate threat to public safety. This must be proven before the usage is made.[160]

Now, the main question of the current analysis is to understand 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 to link 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").[161] Despite being a soft law tool, this instrument aims at addressing the concerns and the potential impacts that the development of advanced technologies (might) have on criminal proceedings and at recalling the safeguards of fundamental rights in this context already elaborated by the ECtHR so that all the actors involved (both judicial and

[160] Ibid.

[161] The European ethical Charter adopted during the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018) is available here.

not) at the national level are well aware of the existing challenging posed by AI as well as of the required delicate balancing of different interests.[162] The key element of the whole instrument is to make clear that when AI tools are employed in judicial proceedings, they shall not violate the right of access to the court and the right to a fair trial (particularly declined as equality of arms and respect for the adversarial process).[163] Among the five principles that the European Ethical Charter addressed, three are worth mentioning for the analysis at stake:

1. The **principle of non-discrimination** which specifically prohibits creating or exacerbating (existing) discrimination between groups and individuals (this can be related to the ethnic origin or religious belief; the socio-economic conditions of the concerned person; sexual orientation or gender identity; or political opinion, among others). For instance, computational systems[164] are well suited to detect the existence of potential discrimination, because the algorithms on which they are based have a set of inputs and are programmed to process specific outputs. Therefore, the potential risk is that these algorithms are subjected to the so-called implicit bias. The levels at which the risks can occur are multiple: for example, if the input is not completely neutral, the output of the processing is at risk of being influenced by bias, which can lead to discrimination against individuals or social groups. Moreover, the algorithm may trivially reproduce unwarranted social biases, since it is designed and interpreted by human beings. This can have

[162] Serena Quattrocolo, *Intelligenza Artificiale e Giustizia: nella Cornice della Carta Etica Europea, gli Spunti per Un'Urgente Discussione tra Scienze Penali e Informatiche*, La Legislazione Penale, 18 December 2018, 3. Available here.

[163] Mitja Gialuz, *Quando la Giustizia Penale Incontra L'Intelligenza Artificiale: Luci e Ombre dei Risk Assessment Tools tra Stati Uniti ed Europa*, Diritto Penale Contemporaneo, 2019, 12. Available here.

[164] To this purpose, computational systems involve the systems that are capable of solving a problem that includes calculations either mathematical or logical, and are able to produce the result as an output.

impacts on the evidence adduced and considered by judges during criminal trials.

2. The **principle of quality and security of data** which, with regard to the analysis of data and judicial decisions, implies the use of certified sources and intangible data. Part of the provision specifically focuses on the security of judicial data processed through computational systems, meaning that the choice of data adduced in criminal trials includes the careful verification of the reliability of the evidence and the integrity of such data, to avoid its (accidental or instrumental) modification. To this purpose, the algorithms underlying the processing must be employed (and safeguarded) in secure environments, to avoid risks to their integrity.
3. The **principle of transparency, impartiality and fairness** entails the accessibility, comprehensibility and external verifiability of the computational processes used for the analysis of judicial data. This is directly linked with the possibility of understanding the computational processes used. With regard to the evaluation of adduced evidence in criminal proceedings, given that the Italian criminal system requires the judge to explicitly provide an assessment of the reliability of each piece of evidence, the "algorithmic transparency" is not in itself sufficient to make clear to the recipients of the decision as well as to the public an effective understanding of the process that led to generating the digital evidence, thus resulting the trustworthiness of the decision as uncertain. To avoid this, the European Ethical Charter suggests the establishment of independent authorities that can verify and certify periodically and *a priori* the tools employed in the justice services.[165] However, for the matter at stake, it is worth mentioning that **Italy, as of today, has not established any**

[165] Quattrocolo, cit, 8.

independent authority responsible to verify *ex-ante* the compatibility of the technological tools (as FRT, such as SARI) with due process guarantees. On the contrary, instead, through the exemptions to the moratorium of the use of FRT in public spaces, Law 205/2021[166] admits the possibility of deploying such tools for the purposes of prevention and suppression of criminal offences (as well as execution of criminal sanctions) without any previous control by the national body that could verify the necessity and proportionality of the concerned measure(s), meaning without even requiring judicial authorities to address the Italian DPA on the matter.

As recalled above, in relation to the use of AI in general, including FRT, within the criminal justice system, the European ethical Charter aims at pointing out the importance of the **accessibility of algorithms to ensure the effectiveness of the right of defence and due process guarantees.**[167]

[166] See above para 2.4.

[167] See above para 2.1. focusing on the Italian principles and para 4.1 related to the ECHR' safeguards.
Antonella Massaro, Angelo Giraldi, Lorenza Grossi, Laura Notaro, Pietro Sorbello, Università degli Studi "Roma Tre", *Intelligenza Artificiale e Giustizia Penale*, December 2020, 136. Available here.

4. European Court of Justice 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 (actual or potential) employment of FRTs by LEAs to prevent and prosecute crimes raises the issue of the compliance of such use with fundamental rights. The mere processing of this data in itself entails an interference with an individual's fundamental rights, regardless of its subsequent actual use and deletion from the authorities' database.

The analysis in this section will focus on the rights protected by the EU Charter of Fundamental Rights (the "Charter") and its interpretation by the Court of Justice of the European Union ("CJEU"). In light of the aim of the research, and considering that the collection and analysis of footage of individuals involve the processing of personal data, the right to privacy (Article 7 of the Charter), and the right to respect personal data (Article 8 of the EU Charter) will be analysed first.

Given the great impact of FRTs on daily lives of human beings, both as individuals and as groups, the analysis will also address whether the use of FRTs has any impact on Articles 11 and 12 of the Charter, which safeguard - respectively - the freedoms of expression and association. The research will also focus on Article 21 of the Charter, due to the potential risks of discrimination inherent in the use of algorithms.

Furthermore, the research will focus on the guarantees and rights that the Charter ensures to individuals subjected to data processing, enshrined in Article 41 of the Charter, which protects the right to good administration, and in Article 47 of the Charter, protecting the right to an effective remedy.

After analysing the main fundamental rights possibly affected by FRTs, the question will be raised as to whether the compression of these rights is legitimate or not. An attempt will be made to establish whether such restrictions can be

operated in compliance with the principle of legality (rule of law) and proportionality enshrined in Article 52 of the Charter.

Finally, the research will consider the compliance of the FRTs with the relevant provisions outlined in the GDPR and in the LED, highlighting the critical elements of the Italian context.

4.1 Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

Article 7
Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
1. Everyone has the right to the protection of personal data concerning him or her. *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rect*ified. *3. Compliance with these rules shall be subject to control by an independent authority.*

As mentioned above,[168] FRTs may constitute a dangerous intrusion into an individual's right to privacy and protection of personal data. To identify the potential

[168] See para. 4.2.

impact of FRTs on the rights protected under Articles 7 and 8 of the Charter, a premise is worth mentioning.

The right to privacy is enshrined in article 7 of the Charter. It corresponds to article 8 ECHR and, in accordance with article 52 (3),[169] it must be interpreted in conformity with it. Article 8 of the Charter specifically addresses the right to protection of personal data, while in the Convention there isn't a corresponding prevision. However, the ECtHR subsumed the right to data protection under Article 8 ECHR, giving a broad interpretation of the concept of "private life."[170]

The close correlation between the two rights (i.e., Art. 8 ECHR and Art. 7 CJEU) has led the CJEU's former Advocate General, Eleanor Sharpston, to define the first as the "classic" right to privacy and the latter as the "modern" right to data protection.[171] The contiguity between the two rights also emerges from the Explanation in the Charter itself, which states that Article 7 is based in particular on Article 8 ECHR, which governs the right to private and family life.[172] Even in *Promusicae v. Telefonica de España* (2008) the CJEU seems to create a new fundamental right encompassing both rights under consideration, "namely the right that guarantees protection of personal data and hence of private life."[173]

---

[169] EU Charter of Fundamental Rights, Article 52 (3): "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection".

[170] European Court of Human Rights, *Amann v. Switzerland*, Application no. 27798/95, 16 February 2000, §65. Available here.

[171] Court of Justice of the European Union, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert,* Opinion of Advocate General Sharpston, 17 June 2010, §71.

[172] Francesco Rossi Da Pozzo, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, rivista Eurojus, 2018, 15. Available here.

[173] Court of Justice of the European Union, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Opinion of Advocate General Kokott, 18 July 2007, §63. Available here.

The CJEU case law considered the right to privacy to be at the core of data protection law, broadly interpreting the concept of "private life", including the protection of personal data[174] (as already done by the ECtHR). According to the definition provided by the European Commission, "[p]ersonal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which are collected together that lead to the identification of a particular person, also constitute personal data."[175] Personal data also includes information known as biometric data. A clear definition of such category is provided by Article 3 (13) of the LED,[176] which describes them as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[177] Amongst others, the analysis of biometric data can provide information on racial or ethnic origin, health conditions, religion, and daily life habits.

It is worth mentioning that the processing of data is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

[174] Court of Justice of the European Union, Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert*, 9 November 2010, §52. Available here.
[175] European Commission, *What is personal data?, Answer*. Available here.
[176] 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, 4 May 2016. Available here. The LED is considered as *lex specialis* to the regulation on the use of FRT.
[177] EPDB, *Guidelines 05/2022 on the use of FR technologies in the area of law enforcement*, 12 May 2022, 17. Available here.

or otherwise making available, alignment or combination, blocking, erasure or destruction."[178]

That being said, the development of new technologies has significantly increased the possibilities of collecting, processing, and analysing personal data of individuals, including biometric data, in potential violation of the rights at stake. These rights, however, are not absolute and "must be considered in relation to their function in society."[179] Specifically, the Articles at stake, as well as Article 52 of the EU Charter, allow for lawful interference with the concerned rights, if certain requirements are met.

As mentioned above, according to Article 52 (3) of the EU Charter, the rights recognised and safeguarded both by the EU Charter and the ECHR, such as the right to private life under Article 7 of the Charter, must be interpreted in accordance with "the meaning and the scope" of Article 8 ECHR. As the Explanation of the Charter clearly stated,[180] this implies that the exemptions to the right to privacy in Article 8 (2) ECHR also apply with reference to Article 7 of the Charter.[181] In particular, "there shall be no interference by a public authority with the exercise of this right **except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime,**

[178] Directive 95/46/EC recital 28, and Regulation (EU) 2016/679. See Court of Justice of the European Union, Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 3 May 2014, §28. Available here.
[179] Court of Justice of the European Union, Case C-291/12, *M. Schwarz v. City of Bochum*, 17 October 2013, §33. Available here
[180] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 52, OJ C 303, 14.12.2007. Available here.
[181] See para 3.2.

for the protection of health or morals, or for the protection of the rights and freedoms of others."[182]

When it comes to lawful interference with the rights safeguarded by Article 8 of the Charter, according to para (2), an interference is deemed justified if the data subject has given their informed consent, or if the law provides for such a compression.

Jurisprudence has long dealt with the characteristics of consent for it to be considered validly given. The definitional problem was solved with the introduction of the GDPR, which states in Article 4(11) that "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"[183] and the same definition is also expressed in Recital 32 of the GDPR.[184] The CJEU then specified that the wording "given his or her consent", meaning active conduct manifested in full knowledge of the facts by the person concerned, "does, however, lend itself to a literal interpretation according to which action is required on the part of the user in order to give his or her consent [...] a user's consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including 'by ticking a box' when visiting an internet website."[185]

[182] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 7, OJ C 303, 14.12.2007, cit.
See also para 4.2 above, with particular attention to the so-called three-part test.
[183] Article 4 (11) GDPR. Available here.
[184] Recital 32, GDPR. Available here.
[185] Court of Justice of the European Union, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, 1 October 2019, §49. Available here.

Furthermore, Article 8 (2) Charter states that the processing of data must be fair and for specific purposes in order to be justified. Fair processing means that "the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data" and that "the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection."[186]

If the conditions required by Article 8 (2) are fulfilled, there is no interference with the concerned right, though the collection, storage or disclosure of such data may still interfere with the right to privacy and be justified.[187]

Article 52 (1) of the Charter encompasses the criteria within which the limitation of fundamental rights can be allowed in EU law. Article 52 (1) (as well as Article 8 (2)) states that fundamental rights can be restricted if "provided for by law" and with respect to the "essence" of those rights and freedoms. The notion of law "includes primary and secondary law; MS legislation - both parliamentary and delegated - and even unwritten MS law, in particular the common law in MS which adhere to it."[188] Furthermore, the law must be in force and legal, meaning "that where an interference is based on Union law its legality can be reviewed incidentally by the CJEU."[189] Finally, "the law must additionally be adequately accessible and formulated with sufficient precision."[190] From the case law of the ECtHR, which is

[186] Explanations relating to the Charter of Fundamental Rights, cit., recital 38.
[187] Juliane Kokott, Christoph Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,* International Data Privacy Law, 2013, Vol. 3, No. 4, 226. Available here.
[188] Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin, *The EU Treaties and the Charter of Fundamental Rights*, Oxford University Press, 2019, 2250.
[189] Ibid.
[190] Ibid.

expressly referred to in the Commentary to Article 52 (1) of the Charter by the complementary nature of the law under consideration, it may be concluded that the requirement of precision brings about as a corollary the foreseeability of the law, as well as the fact that the more serious the interference is, the more precisely the law must be formulated.

In a very recent decision of 2023 (*Ministerstvo na vatreshnite raboti)*[191] the CJEU analysed the requirement of "provided for by law" recalling Article 52 (1) in the context of a tax fraud criminal case in which the defendant had objected to the collection by LEAs of her fingerprint, photographic data and DNA sample. Due to its relevance with regards to principles enshrined in the GDPR and the LED, the contents of the judgments will be analysed below at para 5.7.

Article 52 (1) also requires that limitations to fundamental rights must respect the essence of the right restricted and be proportionate. The restriction “must serve a legitimate aim, be suitable to achieve that aim, be necessary, i.e. be the least restrictive measure available, and it must be proportionate *stricto sensu.*”[192] Regarding the requirement of a legitimate aim of in Article 52 (1), the Explanation of the Charter states that "the reference to the general interests recognised by the Union includes both the objectives set out in Article 3 of the Treaty on European Union and other interests protected by specific provisions of the Treaties,"[193] including the guarantee of an area of freedom, security and justice, the prevention of freedom, security and justice, the prevention and combating of crime.

While the use of FRTs by LEAs could thus be justified by the ultimate objective of preventing and combating crime, it is necessary that it complies with Article 52 (1),

[191] Court of Justice of the European Union, C-205-21, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, 26 January 2023. Available here.
[192] Ibid.
[193] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 52, OJ C 303, 14.12.2007. cit.

which requires that the legislative measures adopted shall "not exceed the limits of what is appropriate and necessary to achieve those objectives."[194] The case law of the CJEU has made clear on numerous occasions that invoking the pursued public interest is *not sufficient* to limit the right enshrined in Article 8 of the Charter (and indirectly that of Article 7 of the Charter).[195] The use of new investigative technologies is indeed very effective to combat grave crimes, such as organised crime and terrorism, but there is a need for clear and precise legislation regulating their scope and requiring "minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."[196]

Furthermore, it must be considered that during the investigation phase the data subject cannot know what data has been processed and on what grounds. Secrecy is indeed an intrinsic trait of such a phase of the criminal trial. If these data were ostensible, i.e. the right of access laid down in Article 8(2) Charter was guaranteed, it could irreparably compromise the efficacy of investigations. Nevertheless, in absence of clear regulation on the matter, the result is an unjustified contraction of Article 8 of the Charter with regards to the data processed during the preliminary investigation phase.[197]

Although there are currently no Court rulings on the use of FRTs concerning the violation of Articles 7 and 8 of the Charter, the principles referred to above may also apply in the present case. Regarding the use of SARI Real-Time, in light of the Court's findings in the various cases examined above, the requirements of

[194]Court of Justice of the European Union, C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 Aprile 2014, §46 (Available here).
[195] Ibid. §51
[196] Ibid. §54
[197] This aspect is also addressed below at para 4.4.

Articles 8 (2) and 52 (1) for the limitation of fundamental rights can not be considered fulfilled for the following reasons:

- as already mentioned with reference to Article 8 ECHR,[198] the use of SARI Real-Time by LEAs and judicial authorities has already been considered by the Italian DPA as **lacking a sufficient legal basis,** as it does not meet the criteria of Article 7 of Legislative Decree 18 May 2018, no. 51;
- even considering the aforementioned law as a legitimate basis for the limitation of the rights at stake, **it does not define the purpose of these limitations in a sufficiently clear and precise manner**;
- the requirement of the **consent of the person concerned cannot help**, given that the person being under investigation is often not even aware that their data is being processed during this phase.

Regarding the use of SARI Enterprise by LEAs and by the judicial authority, we have seen that the same has not been subject to a ban by the Italian DPA. It should be stressed, however, that its use, justified by the ultimate goal of preventing and combating crime, does not *a priori* conform to the parameters set forth in Article 52(1), as the public interest pursued is not sufficient to limit the right enshrined in Article 8 of the Charter (and indirectly that of Article 7 of the Charter). Thus, a case-by-case verification of compliance with the minimum guarantees for the protection of personal data of the individuals involved is necessary.

In conclusion, a brief mention should be made to the issue of processing of data with regards to the prevention/prosecution of terrorism. Recently, the CJEU assessed whether the indiscriminate data retention for combating terrorism, despite its disproportionate impact on fundamental rights and the rule of law, complied with the fundamental rights granted in the EU Charter. In both *Privacy*

[198] See paras. 2.2.1 and 4.2.

International v Secretary of State for Foreign and Commonwealth Affairs and Others[199] and *La Quadrature du Net and Others v Premier ministre and Others,*[200] the CJEU stated that both the EU Privacy and Electronic Communications Directive ("ePrivacy Directive")[201] and the Charter generally prevents national law from enabling indiscriminate retention or transmission of traffic and location data, even if it is for safeguarding national security. However, in *Quadrature Du Net* the CJEU ruled that **indiscriminate data retention measures are lawful if the Member States can prove legitimate and "serious threats to national security."**[202] In such cases, the electronic collection of data can be retained during a strictly necessary period and the decision must be subject to review by a court or independent administrative body.

4.2 Articles 11 and 12 of the Charter of Fundamental Rights of the European Union

Article 11
1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

[199] Court of Justice of the European Union, C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020. Available here.
[200] Court of Justice of the European Union, joined Cases C-511/18, *La Quadrature Du Net and Others and C-512/18 French Data Network and Others*, 6 October 2020 (Available here) and C-520/18, *Ordre des barreaux francophones et germanophone and Others*, 15 January 2020 (Available here).
[201] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available here.
[202] Court of Justice of the European Union, *La Quadrature Du Net*, cit., §§ 136–139, 168.

2. The freedom and pluralism of the media shall be respected.

Article 12

1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.

2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.

The freedom of expression and information is enshrined in Article 11 of the Charter and in Article 10 of the ECHR, and pursuant to Article 52 (3) of the Charter the meaning and the scope of these rights are the same as those interpreted by the ECtHR.[203] According with the Explanation of the Charter, "[t]he limitations which may be imposed on it may therefore not exceed those provided for in Article 10 (2) of the Convention, without prejudice to any restrictions which the competition law of the Union may impose on Member States' right to introduce the licensing arrangements referred to in the third sentence of Article 10(1) of the ECHR."[204]

Article 12 of the ECHR recognises and safeguards the freedom of assembly and association, which corresponds to the same rights enshrined in Article 11 of the ECHR. Article 52 (3) also applies here. It follows that the limitations in Article 11 ECHR also apply to Article 12, i.e. they are only permitted if they are prescribed by law, in pursuance of one of the legitimate purposes expressly listed (e.g. national security, public safety, crime prevention), and are necessary in a democratic society.[205]

[203] See para. 3.3 for the analysis of the ECtHR case law on the right at stake.
[204] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 11, OJ C 303, 14.12.2007, cit.
[205] European Union Agency for Fundamental Rights, *Fundamental rights considerations in the context of law enforcement*, 2020, 29. Available here.

While freedoms of expression and information, as well as of assembly and association, represent crucial cornerstone in a democratic society,[206] there appear to be no previous CJEU decisions on their potential or actual infringement from the use of FRTs (or AI more generally). Nevertheless, the use of these technologies has a profound impact on the rights at stake.

The use of FRT to process facial images captured by cameras in public spaces can interfere with a person's freedom of opinion and expression, as well as freedom of association, including because a necessary aspect of exercising this freedom is group anonymity.[207] This has been defined by the EU Agency for Fundamental Rights ("FRA"), among others, as the **chilling effect of the use of FRTs on the concerned freedoms and rights "**due to fear of the negative consequences that may follow."[208] As a matter of fact, the use of FRTs during demonstrations could potentially discourage people from exercising their rights to freedom of assembly and association, as they may fear being identified and potentially targeted or harassed as a result. This could have a chilling effect on participation in peaceful demonstrations, and could undermine the ability of civil society to engage in peaceful activism and advocacy. Therefore, any deployment of FRTs during demonstrations would need to be carefully scrutinised to ensure that it meets the high standards of necessity and proportionality. This would require balancing the potential benefits of using the technology against the potential negative impacts on the exercise of fundamental rights, including the rights to freedom of assembly and association.

[206] European Court of Human Rights, *Mouvement Raelien Suisse v. Switzerland*, No. 16354/06, 13 July 2012, §48. Available here.
[207] European Union Agency for Fundamental Rights, *Fundamental rights considerations in the context of law enforcement*, cit., 29.
[208] Ivi, 30.

Accordingly, a Court in Germany[209] recognised the mentioned chilling effect of the employment of FRTs on freedoms of association and expression, by observing that individuals that are aware of being subjected to scrutiny in public spaces are led to change their behaviour by not taking part in demonstrations and not fully expressing their thoughts, therefore avoiding to participate in the democratic life of the society. Consequently, the German Court declared illegal the publication on social media of pictures of participants in a demonstration.

Suspecting or, worse, being aware of being subjected to any type of surveillance generates a (consciously or not) change in the behaviour of an individual who is "forced" to adapt the attitudes and - potentially - to refrain from expressing themselves as well as to be discouraged from participating in public demonstrations. Therefore, it is important to carefully consider the potential impacts of FRTs on democratic participation and civil society, and to ensure that any use of such technology is proportionate and respectful of fundamental rights and freedoms.

StraLi is aware of the importance of being able to actively participate in political and social life without the fear of being tracked in one's movements or communications, which is why it has developed a digital guide to protecting one's data and device during a demonstration.[210]

[209] Verwaltungsgericht Gelsenkirchen, 2018, 14 K 3543/18. Available here (in German only).

[210] Guida comoda per situazioni scomode: manifestazione digitale. Available here. (only in italian). The guide is one of the actions StraLi has taken as a partner in the Reclaim Your Face campaign, a European Citizenship Initiative aimed at demanding stringent regulation of facial recognition-based technologies from the European Commission.

4.3 Article 21 of the Charter of Fundamental Rights of the European Union

> *1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.*
>
> *2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.*

Article 21 of the Charter reflects the corresponding right in Article 14 ECHR and Protocol No. 12. This provision prohibits "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic characteristics, language, religion, etc. social origin, genetic characteristics, language, religion religion or belief, political or any other opinion, membership of a national minority, heritage, birth, disability, age or sexual orientation, age or sexual orientation". While Article 14 ECHR lists specific grounds for protection against discrimination, the Charter's right to non-discrimination is open and extends to a wider range of grounds. Additionally, the Charter's right to non-discrimination is a freestanding right, meaning that it applies even in situations not covered by any other provision of the Charter. However, both the ECHR and the EU Charter allow for differential treatment if justified. This means that if differential treatment pursues a legitimate aim and the means used to pursue that aim are necessary and proportionate, it may be allowed.[211]

[211] Court of Justice of the European Union, C-356/12, *Wolfgang Glatzel v. Freistaat Bayern*, 22 May 2014, §43. Available here.

There are no previous CJEU decisions relating to Article 21 and the use of FRTs or AI. However, due to its open formulation and broad reach, it is conceptually fit to tackle cases of algorithmic discrimination. As FRA stated, "[d]iscrimination in data-supported algorithmic decision-making can occur for several reasons. Discrimination can occur during the design, testing and implementation of algorithms used for facial recognition. This is because biases are built into the algorithm itself - consciously or unconsciously."[212] Machine learning works by extracting information from large amounts of data. If this data does not represent a whole and full reality but only a part of it, the algorithm's functioning may be limited (*rectius*: incorrect), because the machine is only able to process a narrow amount of data, due to the limited knowledge of a certain context.

As a way of example, if FR software is trained to identify the presence of a face from images depicting predominantly light-skinned men, it will be more accurate in the predictions for this group of people, than for others. As a consequence, FR algorithms may perform less accurately on people with darker skin tones or of certain ethnicities, which could lead to unfair treatment or discrimination for individuals who belong to those groups. Additionally, if the images used to train the FRT are not representative of the population it is being used on, it could lead to further biases. If there are differences in the performance of an algorithm, it is usually very difficult and sometimes impossible to eliminate biases through mathematical or programmatic solutions.

Among the main causes of bias is quality bias data used to develop algorithms and software. FR softwares have to be fed with large amounts of facial images: the more images of the captured person in the database, the more

[212] European Agency for Fundamental Right, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 27.

accurate the prediction of the algorithm.[213] However, as the EU FRA noted "**accuracy is not only determined by the number of facial images processed, but also by their quality.** Data quality also requires a representative set of faces reflecting different groups of people."[214] To date, most algorithms have been developed with reference to images depicting white men, with the consequence that the somatic features of darker skin tones individuals and/or individuals of different ethnic origins are often difficult to identify, generating a large margin of error.[215] As FRA affirmed, "the complexity of the algorithms makes it harder to identify and remove such biases. Instead of providing objective analysis, predictive policing software may turn into an 'echo chamber' cementing existing systemic flaws and injustices with the 'stamp' of what appears to be scientific legitimacy."[216]

Finally, it is worth mentioning the discriminatory impact of FRTs on migrants and asylum seekers within the Italian context.[217]

During disembarkation and afterwards, migrants and asylum seekers are subjected to compulsory identification procedures (their fingerprints are taken, they receive a bracelet with a progressive identification number which is shown during signalling, and they are given a waybill) without being able to know that the path their personal and biometric data will be taken. As pointed out by Hermes,[218] 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,

[213] Ibid.
[214] Ibid.
[215] Ibid.
[216] European Union Agency for Fundamental Rights, *Getting The Future Right - Artificial Intelligence and Fundamental Rights*, 2020, 70. Available here.
[217] See also para 2.2.1.
[218] Hermes Center for Transparency and Digital Human Rights (Laura Carrer - Riccardo Coluccini) *Technologies for Border Surveillance and Control in Italy. Identification, Facial Recognition, and European Union Funding*, 2021, cit., 19.

fingerprints and personal data also of people under criminal investigation or deemed dangerous or suspicious by public authorities converge. This database is then used in conjunction with the SARI Enterprise FR system, whose algorithms - as mentioned - are harbingers of bias and in particular with regard to darker skin tones individuals or non-Caucasian ethnicity.

It is worth stressing, again, that the use of these technologies without proper oversight and regulation carries a high risk of producing false positives with detrimental consequences, such as being listed on the register of suspects due to an incorrect algorithm match. What is more, when one considers that such consequences can affect particularly vulnerable categories of individuals, such as migrants and asylum seekers, the threshold of attention should be even higher.

4.4 Article 41 of the Charter of Fundamental Rights of the European Union

1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union.

2. This right includes:

(a) the right of every person to be heard, before any individual measure which would affect him or her adversely is taken;

(b) the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy;

(c) the obligation of the administration to give reasons for its decisions.

> *3. Every person has the right to have the Union make good any damage caused by its institutions or by its servants in the performance of their duties, in accordance with the general principles common to the laws of the Member States.4. Every person may write to the institutions of the Union in one of the languages of the Treaties and must have an answer in the same language.*

The right to good administration is a well-established general principle of EU law, which applies to all EU bodies, institutions and agencies, and which requires Member States to respect the right to good administration' standards in all national procedures.[219] Article 41 enshrines "procedural fundamental rights,"[220] whose purpose is to ensure that the administration pays sufficient respect to the rights of individuals by providing for, on the one hand the right to have access to their file. and on the other hand the obligation of any public authority to give reasons for its decisions.

The concerned right allows the interested individual to understand on what grounds a certain measure/action/decision has been taken towards him/her/them. Transparency on such reasons enables the exercise of several related rights, including the right to be heard and the rights to an effective remedy and to a fair trial: only by being aware of the reasons which led to the adoption of a certain measure it is possible to effectively challenge it. Consequently, the right of a person to access their file complements the other rights to defence.

Within criminal proceedings, the right of access to files, also known as the right to disclosure, implies the right of a defendant to access the evidence gathered by the prosecution against them. This right is crucial, because it allows the defendant to prepare their defence, to challenge the evidence presented against him or her,

[219] Court of Justice of the European Union, C-604/12, *H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General*, 8 May 2014, §49. Available here.
[220] Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin, *The EU Treaties and the Charter of Fundamental Rights*, cit., 2205.

and, overall, to ensure the fairness of the trial. Therefore, if the defendant is denied accessing evidence, this can damage his ability to defend himself and can lead to an unfair trial. On the other hand, the principle of confidentiality (*principio di segretezza*) is based on the fact that certain information should be kept confidential and not disclosed to the public, otherwise the effectiveness of the criminal investigation would be jeopardised.

Also, this principle is particularly significant during criminal investigations because it helps protect the privacy of people who may be investigated. Nonetheless, it is important to balance the right of access to files with the principle of non-disclosure. In some cases, it may be necessary to keep sensitive information confidential to protect the investigation or the privacy of those involved. In such cases, the court may limit the defendant's right to access certain evidence. It is the court's responsibility to ensure that the balance between the right at stake and the principle of non-disclosure is maintained fairly and protects the rights of all the parties involved. However, in the CJEU's interpretation, the scope of the right to access enshrined in Article 41 appears to refer only to those documents that form the basis of the decision and are deemed necessary for the formulation of the defence (accordingly, it also imply that the defence does not have the right to access documents or information concerning individuals involved in the same procedure *other* than the one(s) they represent).[221]

According to the CJEU, “the contested measure clearly discloses the essential objective pursued by the institution”[222] and the statement of reason in the judgement “must disclose in a clear and unequivocal fashion the reasoning followed by the institution which adopted the measure in question in such a way

[221] Ivi, 2206

[222] Court of Justice of the European Union, Joined Cases C-78-79/16, *Pesce and Serinelli*, 9 June 2016, §90. Available here.

as to enable the persons concerned to ascertain the reasons for the measure and to enable the competent Court of the European Union to exercise its power of review."[223]

As the mentioned principles apply to national (and supranational) decisions, it is clear that **the right to good administration also applies when AI systems (including FRTs) process personal data and support the decision-making process of public authorities, such as the ones involved in the criminal trial.** In this case the complexity lies in two aspects. On the one hand, balancing the secrecy of the investigation with the right to know whether one's data is retained on file and for what reason. On the other hand, should it be possible to gain access to this information, the number of requests from stakeholders could be potentially enormous.[224] However, according to research published by FRA, the storage and processing of individuals' faces often takes place without their knowledge, which makes it impossible for them to access their data and possibly request its modification or deletion.[225]

The European Data Protection Board ("EDPB")[226] has clarified the obligation of Member States "to inform individuals of existing video surveillance devices. Such information should be provided through a warning sign at a reasonable distance from the monitored places, and information that is accessible without entering the area under surveillance. This may include an information sheet, a link to a website

[223] Court of Justice of the European Union, Case C-131/15 P, *Club Hotel Loutraki*, 21 December 2016, §46. Available here.
[224] European Union Agency for Fundamental Rights, *Getting The Future Right - Artificial Intelligence and Fundamental Rights,* cit., 81.
[225] European Union Agency For Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 31
[226] European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices – version for public consultation*, Brussels, 10 July 2019, 21-23. Available here.

detailing information on the surveillance, a telephone number to receive further information, or an app mapping the location of video devices."[227]

However, according to FRA, one of the biggest problems concerns **the lack of awareness and understanding of exercising the right to access, correct or delete inaccurate personal data stored in large-scale IT systems, as well as facial recognition databases used for law enforcement purposes.** Moreover, very few lawyers specialise in this area, which makes the protection of these rights even more difficult.

4.5 Article 47 of the Charter of Fundamental Rights of the European Union

1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

2. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

3. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

[227] European Union Agency For Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 25.

4.5.1 Article 47(1)

Article 47 of the Charter guarantees the right to an effective remedy before a tribunal in case of violations of rights and freedoms protected by EU law. According to the CJEU,

> the principle of effective judicial protection is a general principle of Community law stemming from the constitutional traditions common to the Member States, which has been enshrined in Articles 6 [right to a fair trial] and 13 [right to an effective remedy] of the ECHR and has also been reaffirmed by Article 47 of the Charter of Fundamental Rights of the European Union.[228]

From this follows that, when interpreting the meaning of the right to an effective remedy under Article 47, it is important to bear in mind the ECtHR jurisprudence on the aforementioned rights.

First of all, it should be specified that even if the right to an effective remedy corresponds to Article 13 ECHR, the scope of the two rights is different: while the latter enshrines the right to "an effective remedy before a national authority" for "claims based on" ECHR-protected rights, Article 47 CJEU has a broader scope, providing for a remedy before a "tribunal" and applying to all rights included in EU law.[229]

Neither the ECHR nor the Charter define the term “remedy”, nor they provide specific guidance on when a remedy can be considered as effective. However, through the CJEU’s case-law, it is possible to draw the boundaries of this right. While it is on Member States to establish national systems of remedies and legal

[228] Court of Justice of the European Union, T-49/07, *Sofiane Fahas v. Council of the European Union*, 7 December 2010, §59. Available here.
[229] Ibid.

procedures to comply with the right at stake, EU law requires that domestic legislations ensure effective judicial protection, by respecting European standards, and therefore not undermining such right.[230] In this sense, the CJEU emphasised that the remedies provided by States to ensure effective judicial protection in areas governed by EU law "are no less favourable than those governing similar domestic actions (principle of equivalence) and do not make it in practice impossible or excessively difficult to exercise the rights conferred on consumers by European Union law (principle of effectiveness)."[231]

The CJEU considers the notion of "tribunal" to be met when "the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent."[232]

Article 47 also includes the right to be advised, defended and represented, which guarantees a fair trial in the light of the CJEU's jurisprudence recalling the ECtHR's case-law[233] on Article 6. The principle of fair trial was extensively analysed in section 2.1.1 of this research.

[230] This has been also clarified by the Court of Justice of the European Union in the *Unibet (London) Ltd, Unibet (International) Ltd v. Justitiekanslern* case, C-432/05, 13 March 2007, above, in which the Court stated that the characteristics of a remedy must be determined in a manner that is consistent with the principle of effective judicial protection.

[231] Court of Justice of the European Union, C-415/11, *Mohamed Aziz v. Caixa d´Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa)*, 14 March 2013, §50. Available here. See also CJEU, Joined cases C-482/13, C-484/13, C-485/13, C-487/13, *Unicaja Banco SA v. José Hidalgo Rueda and Others, Caixabank SA v. Manuel María Rueda Ledesma and Others, Caixabank SA v. José Labella Crespo and Others and Caixabank SA v. Alberto Galán Luna and Others*, 21 January 2015. Available here.

[232] Court of Justice of the European Union, C-54/96, *Dorsch Consult Ingenieurgesellschaft mbH c. Bundesbaugesellschaft Berlin mbH*, 17 September 1997, §23. Available here.

[233] According to the case-law of the ECtHR, "the concept of a fair trial referred to in Article 6 of the ECHR consists of various elements, which include, inter alia, the rights of the defence, the principle of equality of arms, the right of access to the courts, and the right of access to a lawyer both in civil and criminal proceedings ", see Court of Justice of the European Union, C-305/05, *Ordre des*

That being said, according to the CJEU

> the right to effective judicial protection is not an absolute right and that, in accordance with Article 52(1) of the Charter, limitations may be placed upon it, on condition that (i) those limitations are provided for by law, (ii) they respect the essence of the rights and freedoms at issue, and (iii) in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[234]

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 that provides that "if the person accused of an intentional offence subject to public prosecution refuses to cooperate voluntarily in the collection of the biometric and genetic data concerning him or her in order for them to be entered in a record, the criminal court having jurisdiction must authorise enforcement of their collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which they are accused."[235] Under Bulgarian law, a person is considered formally charged if there are "sufficient evidence that they are guilty of an offence subject to public prosecution is gathered"[236] and that the accusation can take place at any time during the preliminary procedure (the so-called *fase delle indagini preliminari* under the Italian Code of Criminal Procedure) during which evidence is

barreaux francophones et germanophone and others v. Conseil des ministres, 26 June 2007, §31. Available here.

[234] Court of Justice of the European Union, C-205/21, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, cit., §89.

[235] Ivi, §77.

[236] Ivi, §78.

gathered. It is only at the end of this phase, i.e. at the time of disclosure, that the person concerned becomes aware of the elements of the charge against them and present the defence. The critical point of the case is that the Bulgarian legislation does not "confer on the court which authorises collection of the biometric and genetic data concerning the accused person in order for them to be entered in a record jurisdiction to assess the evidence on which that accusation is founded, a power which lies with the authorities handling the investigation."[237] The CJEU recalls that any accused person who has objected to the collection of their biometric data is entitled to an effective remedy before a court against the decision to authorise the coercive implementation of this collection. In particular,

> that safeguard entails the court with jurisdiction having the ability to verify that the measure accusing the person concerned that constitutes the legal basis for the creation of the police record has been adopted – in accordance with the rules of national criminal procedure – in the light of sufficient evidence that he or she is guilty of an intentional offence subject to public prosecution.[238]

The CJEU also points out that the limitation to the right to personal data must, firstly, be prescribed by law (a circumstance fulfilled in the present case), and secondly, that the essential content of the right to an effective remedy must be respected. Such a right includes, *inter alia*, the right of the data subject to bring an incidental action before a court if there is no direct judicial remedy to challenge the measure.[239] This condition is deemed fulfilled if it is possible to verify that biometric and genetic data have not been obtained in violation of rights guaranteed by EU law at the judicial stage following the investigation phase, which is characterised

[237] Ivi, §80.
[238] Ivi, §88.
[239] Ivi, §94.

by the principle of confidentiality, or if other administrative or extrajudicial remedies are available in the absence of the judicial stage. The CJEU therefore concludes that "[i]t may prove justified, during the preliminary stage of the criminal procedure, to shield temporarily from judicial review the assessment of the evidence on which accusation of the person concerned, and therefore the collection of his or her biometric and genetic data, is founded. Such review, at that stage, might impede the conduct of the criminal investigation in the course of which those data are being collected and excessively limit the investigators' ability to clear up other offences on the basis of a comparison of those data with data gathered during other investigations. That limitation of effective judicial protection is therefore not disproportionate, provided that national law subsequently guarantees effective judicial review."[240]

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. AI systems must always remain under human control and Member States must investigate possible responsibilities, attributable to humans, that may arise in the development or use of AI systems. In this regard, anyone who suspects to have been subjected to a measure based on results obtained through and with the support of AI technologies should (*rectius*: must) be able to turn to a judge to examine the legitimacy of the measure.[241]

The critical point, as analysed in the judgement, revolves around the question of the **substantial impossibility for the person whose data is being processed to be aware of the reasons for the processing during the preliminary investigation phase**, in light of the alleged endangering of the secrecy thereof.

[240] Ivi, §100.

[241] Council of Europe Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights* – Recommendation, Council of Europe, Strasbourg, May 2019, 13. Available here.

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 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Other,*[242] the CJEU held that in case of security measures affecting the right to privacy and the protection of personal data, national authorities must inform the persons concerned about the processing of their images, **when such information is no longer able to affect the development of the investigation.** Such a situation can arise when LEAs compile a "watchlist" of FR with a large amount of facial images. According to the CJEU, it is only through notification by the authorities to the individuals included in these lists that they can exercise their right to an effective remedy by requesting the reasons for the processing.[243] As will be further analysed in Section 5.7, both the GDPR and the LED reiterate that the right to an effective judicial remedy must be guaranteed on decisions of the controller or processor[244] as well as the supervisory authority.[245] According to FRA, "*it is crucial to note that* ***the possibility to lodge an administrative complaint before a supervisory authority as provided for by the GDPR*** **(art. 77)** ***and the LED*** **(art. 52)** ***is not considered an effective judicial remedy under Article 47 of the Charter,*** *since no court is involved in*

[242] Court of Justice of the European Union, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, §121. Available here.
[243] European Union Agency For Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit, 32.
[244] Law Enforcement Directive, Art. 54; and GDPR, Art. 79
[245] Law Enforcement Directive, Art. 53; and GDPR, Art. 78

such a review."[246] If internal data access mechanisms are unable to resolve disputes, the individual must have access to effective judicial redress before a supranational court.[247]

4.5.2 Article 47(2)

Article 47(2) provides for the right to fair proceedings, the corollaries of which are the principle of equality of arms or procedural equality.[248] This principle, as already analysed in section 2.1.1, implies the right to an adversarial trial, and the right to be heard and have an effective defence. In the light of the focus of this research, this analysis will be limited on these two rights, without considering the case-law on a fair and public hearing within a reasonable time, as well as the last paragraph of Article 47 on legal aid.

As the CJEU stated, "in all proceedings initiated against a person which may well culminate in a measure adversely affecting that person, respect for the rights of the defence is a fundamental principle of EU law which must be guaranteed even in the absence of any rules governing the proceedings in question. That principle requires that the addressees of decisions that significantly affect their interests **be placed in a position in which they may effectively make known their views on the evidence on which the contested decision is based.**"[249] According to

[246] European Union Agency For Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit, 32.
[247] Council of Europe, *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence*, 26 June 2019, para. 4.5. Available here.
[248] Court of Justice of the European Union, Joined Cases C-514/07 P, C-528/07, *Kingdom of Sweden v Association de la presse internationale ASBL (API) and European Commission (C-514/07 P), Association de la presse internationale ASBL (API) v European Commission (C-528/07 P) and European Commission v Association de la presse internationale ASBL (API) (C-532/07 P),* 21 September 2010, §88. Available here.
[249] Court of Justice of the European Union, Case C-418/11, *Texdata Software GmbH*, 26 September 2013, §83. Available here.

the CJEU, "if the judicial review guaranteed by Article 47 of the Charter is to be effective, **the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either by reading the decision itself or by requesting and obtaining notification of those reasons**, without prejudice to the power of the court with jurisdiction to require the authority concerned to provide that information."[250]

As already stated with reference to the first paragraph of Article 47, the adversarial principle may also be restricted, such as if "in exceptional cases, a national authority opposes precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken"[251] by invoking the reason of State' security. In such cases, however, it is for the national court to balance those reasons of general interest while ensuring "sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle"[252] by limiting interference in the exercise of that right to what is strictly necessary.[253] The above considerations with regard to the possibility of knowing whether and which personal data have been processed during preliminary investigations also apply with regard to the paragraph under consideration.

Despite the absence of specific CJEU jurisprudence on the issue at hand, the considerations already made in section 2.1.1 apply here. Specifically, the complexity and opacity of AI systems interfere with the right to equality of arms and a fair trial, even only for the fact that the accused person is, more often than not, not even aware that they are subject to the processing of their data, a circumstance that implies the impossibility of challenging the decision or finding evidence in their

[250] Court of Justice of the European Union, Case C-300/11, *ZZ v Secretary of State for the Home Department*, 4 June 2013, §53. Available here.
[251] Ivi, §57
[252] Ibid.
[253] Ivi, §64.

favour. Often the functioning of such systems by means of algorithms is not explicable because the subject cannot know, step by step, how such systems work, as there is often an obscure "black box."[254] This means that it is not possible to trace backwards the operation of certain mechanisms used by FRT: one cannot challenge - i.e. have a right to an effective remedy - what they do not know.

In conclusion, it is relevant to briefly mention Article 49 of the Charter, which enshrines the principle of legality and proportionality of criminal offences and penalties, and in particular its corollary of the principle of foreseeability. This principle implies that criminal provisions must be clear and precise so as to guide the choices of the individual, who must be aware that, by committing an action or omitting an act, they may commit a criminally relevant act. The use of FRTs within the Italian criminal justice system lacks a precise national legal basis authorising this type of processing. As already said, the problem arises because both the GDPR and the LED require the existence of a national law that specifically provides for the modalities of the processing as a prerequisite for the legitimacy of the processing of biometric data for the investigation and prosecution of crimes. The law should not merely authorise the processing per se (the *"an"*), but should ensure the widest respect of fundamental rights. It should regulate the modalities of the processing (the *"quomodo"*), as well as provide for internal control systems for the use of such technologies. This aims to ensure that the risk of abuse is reduced.[255] Such a solid regulatory basis, as repeatedly stated, is lacking in the Italian landscape, making the fundamental rights of the individual vulnerable.

[254] Elettra Currao, *Facial recognition and fundamental rights: setting the balance,* Diritto penale e uomo, fascicolo 5/2021, Diritto penale e uomo, fascicolo 5/2021, Maggio 2021, 80. Available here (italian version).
[255] Ivi, 87.

4.6 The GDPR and the LED Directive

Besides the safeguards contained in the EU Charter, it is essential to focus on specific regulations that the EU has adopted throughout the years to better govern tools and means that can affect the right to privacy and to ensure data protection, namely the LED and the GDPR of 2016. Both the LED and the GDPR are applicable to the automated processing of personal data and to manual processing that is part of a filing system, as stated in Article 2(1) of both regulations. However, the LED is a more specialised regulation (*lex specialis*) that applies when public authorities process personal data for the prevention, investigation, detection, or prosecution of criminal offences, as stated in Recitals 11 and 12 of the LED and Recital 19 of the GDPR. Accordingly, **the processing of facial images must adhere to the primary legal principles of data protection, such as being lawful, fair, and transparent, having a specific, explicit, and legitimate purpose, and following data minimization, data accuracy, storage limitation, data security, and accountability requirements**, as outlined in Article 5 of the GDPR and Article 4 of the LED. Controllers must take appropriate measures to provide information related "to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12 GDPR).

Article 6 LED

> obliges the Member States to provide for the controller, "where applicable and as far as possible", to make a clear distinction between personal data of different categories of data subjects, such as those referred to in Article 6(a) to (d), namely, respectively, persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; persons convicted of a criminal offence; victims

> of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and, finally, other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in Article 6(a) and (b)."[256]

Therefore, Member States must distinguish between the data of the different categories of data subjects so that "they are not subject without distinction – whatever the category to which they belong – to same degree of interference with their fundamental right to the protection of their personal data,"[257] including persons suspected of having committed a criminal offence (ex Article 6(a) LED) . Although the obligation to make this distinction is not absolute, as the provision provides for it "where applicable and as far as possible", and does not provide an exhaustive list of the persons concerned,[258] the CJEU considers that "national legislation which provides for the compulsory collection of biometric and genetic data of natural persons in order for them to be entered in a record, where sufficient evidence is gathered that the person concerned is guilty of a criminal offence, appears consistent with the objective of Article 6(a) of Directive 2016/680."[259]

The transparency principle (Article 5(1)(a) GDPR) requires that individuals be made aware of the collection, use, and processing of their personal data and the extent to which it will be processed (Recital 39 GDPR). However, this does not prohibit competent authorities from conducting covert investigations or video

[256] Court of Justice of the European Union, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* cit., §82
[257] Ivi, §83.
[258] Ivi, §84
[259] Ivi, §85.

surveillance (Recital 26 LED). Member States may create exceptions to Article 13(3) LED (which regulates the information to be given by the controller to the data subject) in order to avoid obstructing ongoing investigations or to protect public and national security. These exemptions may be crucial for law enforcement, as revealing the use of FRTs to suspects could compromise their efforts. However, since such exemptions can impede data subjects from exercising their rights, *strong justifications* are required for their use. To meet transparency requirements for video surveillance under the GDPR, the EDPB suggests a two-tiered strategy. Firstly, a warning sign must be prominently displayed in a position that the (potential) data subject can easily discern the conditions of the surveillance before entering the monitored area.[260] This sign should convey the most critical information. Secondly, other necessary information may be conveyed via other readily available methods, such as posters and websites, which should be explicitly referenced on the first layer through a QR code or website address.[261] Moreover, it is essential to have a specific, clear, and lawful purpose for any video surveillance activity.

The data minimisation principle, as outlined in the GDPR and LED, requires that the amount of data collected should be restricted or not excessive for its intended purpose (Article 5(1)(c) GDPR and Article 4(1)(c) LED). However, the European Data Protection Supervisor ("EDPS") highlights that FRTs systems may not comply with this principle.[262] Additionally, both the GDPR and LED incorporate the storage limitation principle, which mandates that personal data must not be kept in an

[260] European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices – version for public consultation*, Brussels, 10 July 2019, cit., 22.
[261] Ivi, 23.
[262] Wojciech Wiewiórowski, *Facial recognition: A solution in search of a problem?*, European Data Protection Supervisor, 2019. Available here.

identifiable form beyond the time required for the intended processing purpose (Article 5(1)(e) GDPR and Article 4(1)(e) LED).

To ensure lawful processing, specific legal requirements must be met, as outlined in Recital 40 GDPR and Recital 35 LED. Video surveillance may have a legal basis in Article 6 GDPR or in national transpositions of Article 8 LED, but if it involves special categories of data, the processor must also meet the strict requirements of Article 9 GDPR or Article 10 LED. Based on Article 6 of the GDPR and Article 8 of the LED, video surveillance can be justified "for the purposes of the legitimate interests," including crime prevention, but if it involves processing special categories of data, the processor must also comply with the strict requirements outlined in Article 9 GDPR or Article 10 LED. However, article 9 GDPR and Article 10 LED - which will be analysed in full in the following paragraphs with reference to the CJEU judgement of 2023 - have a different scope of application related to data processing. Indeed,

> [W]hilst processing of biometric and genetic data by the competent authorities for purposes covered by Directive 2016/680 may be allowed provided that, in accordance with the requirements laid down in Article 10 thereof, it is strictly necessary, is subject to appropriate safeguards and is provided for by EU or Member State law, that will not necessarily be true of processing of such data that falls within the scope of the GDPR.[263]

As a matter of fact, Article 9 (1) of the GDPR forbids the processing of personal data revealing “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, as well as the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning the

[263] Court of Justice of the European Union, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* cit., §63.

health or sex life or sexual orientation of a person", but this prohibition is lifted in the case of, among others, the use of such data in the course of criminal investigations or during border controls.[264] The EDPB considers that "the use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent from all data subjects (Article 9(2)(a) GDPR) however another suitable exception in Article 9 could also be applicable."[265]

According to Article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is *"***necessary for reasons of substantial public interest,** on the basis of Union or Member State law which **shall be proportionate to the aim pursued,** respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Although slightly more liberal, similar conditions are outlined in Article 10 of the LED.[266] The burden of proof related to the fulfilling of the requirements set by Article 9 (2) (g) remains on the data controllers because the two legal bases ("explicit consent" or "processing necessary for grounds of substantial public interest") represent exceptions to the GDPR's prohibition on the processing of biometric data (as per Article 9(1)).

Within law enforcement contexts, police departments typically invoke criminal procedure codes, surveillance codes and police laws as their legal bases. In a German case, the Hamburg Data Protection Authority (DPA) considered that indiscriminate video surveillance and subsequent biometric extraction and storage

[264] European Union Agency For Fundamental Rights, *Handbook on European data protection law,* 2018 Edition, 160. Available here.
[265] European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices – version for public consultation*, Brussels, 10 July 2019, cit., 15.
[266] For a more elaborated and detailed presentation of the necessity and proportionality test under European law, consult FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, 35-38. Available here.

during the 2017 G20 Summit, lacked sufficient legal bases, in violation of Art. 8 (2) EU Charter.[267]

As established by the CJEU in the recent *Ministerstvo na vatreshnite raboti*, national courts are responsible to verify

> whether the dual reference to Article 9 of the GDPR and to the provision of national law which transposes Article 10 of Directive 2016/680 may be justified by the fact that the scope of the provision of substantive law containing such a dual reference covers all the activities of the departments of the Ministry of the Interior.[268]

Moreover, the referring court must

> satisfy itself that, in particular so far as concerns the provision of substantive law which furnishes a legal basis for the collection of biometric and genetic data in the context of creation of a police record, the set of relevant provisions of national law may be interpreted, in accordance with EU law, as making apparent, in a sufficiently clear, precise and unequivocal manner, in which cases the rules of national law transposing the directive at issue apply and in which cases it is the rules of the GDPR that are relevant.[269]

The CJEU concludes by stating that Article 10(a) of Directive 2016/680, interpreted in light of Article 52 of the Charter, shall be interpreted

[267] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg,* 2018 (German version only).
[268] Court of Justice of the European Union, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, cit., §75.
[269] Ibid.

> as meaning that the processing of biometric and genetic data by the police authorities with a view to their investigative activities, for purposes of combating crime and maintaining law and order, is authorised by Member State law, within the meaning of Article 10(a) of Directive 2016/680, p*rovided that the law of that Member State contains a sufficiently clear and precise legal basis to authorise that processing.*[270]

In this regard, it is important to stress again that the Italian DPA, in its decision of 25 March 2021, considered that the articles of the Italian Code of Criminal Procedure and the other regulations invoked by the Ministry of the Interior could not constitute a valid legal basis for the use of SARI Real-Time. Consequently, they could not legitimately authorise the processing of biometric data in accordance with Article 9 of the GDPR.[271]

As part of the *Ministerstvo na vatreshnite raboti* ruling, the ECJ was called upon to determine whether Article 10 LED, referring to the processing of biometric data, precludes national legislation

> which provides for the **systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution** in order for them to be entered in a record, without laying down an obligation on the competent authority to determine and to demonstrate, first, that their collection is necessary for achieving the specific objectives pursued and, second, that those objectives cannot be achieved by collecting only a part of the data concerned.[272]

[270] Ivi, §76.
[271] See para 2.2.1.
[272] Court of Justice of the European Union, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, cit., §114.

As reflected in the ECJ's case-law, the purpose of this article "is to ensure enhanced protection with regard to that processing"[273] which, due to the "particular sensitivity of the data at issue and the context in which they are processed"[274] leads to "significant risks to fundamental rights and freedoms, such as the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter."[275]

Moreover, according to the ECJ the requirement that the processing of such data is authorised "only if strictly necessary" (Art. 10 LED) must be interpreted as laying down *enhanced* conditions for the lawfulness of the processing of sensitive data.[276] The purposes of the processing of biometric and genetic data cannot, therefore, be designated in excessively general terms, requiring, on the contrary, a sufficiently precise and concrete definition to enable the "strictly necessary" nature of such processing to be assessed with a particularly strict control of compliance with the principle of data minimisation.[277]

In light of the above considerations, the ECJ concluded that national legislation which provides for the systematic collection of biometric and genetic data of any person formally charged with an intentional offence indictable by a national court is contrary, in principle, to the requirement set out in Article 10 of the LED, since

> [s]uch legislation is liable to lead, in an indiscriminate and generalised manner, to collection of the biometric and genetic data of most accused persons since the concept of 'intentional criminal offence subject to public

[273] Ivi, §116 and Court of Justice of the European Union, C-136/17, *GC and Others (De-referencing of sensitive data),* 24 September 2019*,* §44*. Available here.*
[274] Ibid.
[275] Ibid.
[276] Court of Justice of the European Union, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, cit., §117.
[277] Ivi, §§124-125.

> prosecution' is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity.[278]

Indeed,

> the mere fact that a person is accused of an intentional criminal offence subject to public prosecution cannot be regarded as a factor that in itself enables it to be presumed that the collection of his or her biometric and genetic data is strictly necessary in the light of the purposes that it pursues and given the resulting interference with fundamental rights, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.[279]

It is, thus, for the national court to determine whether the domestic legislation permits an assessment of the "strictly necessary" nature of the collection of both biometric data and genetic data of the person concerned, for the purposes of their registration, taking also into account the nature and gravity of the offence.[280] Therefore, there is an obligation on the competent national authority to verify and demonstrate that the collection of biometric data is strictly necessary to achieve the objectives pursued (i.e., the prevention and suppression of crime) and that those objectives cannot be achieved by measures involving less interference with the rights and freedoms of the person concerned.

Similar requirements, as mentioned, are also provided by the GDPR. For instance, the necessity and proportionality principles enshrined in Article 9 GDPR must be applied in this context by taking all necessary steps to comply with them. This implies that prioritisation must be given to FRTs solutions that are most in line with

[278] Ivi, §129.
[279] Ivi, §130.
[280] Ivi, §132.

such standards on the processing of personal data (for example, and to the greatest extent possible, FR systems that employ verification functionality rather than identification).

As already mentioned, the LED was given application in Italy with Legislative Decree 51/2018 (hereinafter "d.lgs. 51/2018"). The discipline provided for the LED and the applicative Legislative Decree must be analysed by taking into consideration also the pre-existing regulation (established by Presidential Decree) regarding the processing of data for police purposes (Decreto del Presidente della Repubblica 15 gennaio 2018, n.15, hereinafter "d.P.R. 15/2018"). The following table summarises and compares the most important provisions of this layered legal framework.

DIRECTIVE	**ITALIAN IMPLEMENTATION**
Art. 6, Distinction between different categories of data subject Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as: (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;	**Art. 4, d. lgs. 51/2018**, ***Conservazione e verifica della qualità dei dati, distinzione tra categorie di interessati e di dati (*****Retention and verification of data quality, distinction between data subject and data categories)** The distinction applies to: *persone sottoposte a indagine;* *imputati;*

(b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).	*persone sottoposte a indagine o imputate in procedimento connesso o collegato;* *persone condannate con sentenza definitiva;* *persone offese dal reato;* *parti civili;* *persone informate sui fatti;* *testimoni.* According to Mobilio, "this distinction enshrined in terms of principle, however, is not followed by a discipline properly modelled on it, with the result that there are no conditions to be met for the processing of data in relation to different subjects, **who find themselves being treated indiscriminately in the same way.**"[281]
Art. 4. para.2 Processing by the same or another controller for any of the purposes set out in Article 1(1) [*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,*	**Art. 13, d.P.R. *Comunicazione dei dati a pubbliche amministrazioni o enti pubblici e a privati* ("Disclosure of data to public administrations or public bodies and to private individuals")**

[281] Mobilio, cit., 157.

including the safeguarding against and the prevention of threats to public security] other than that for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.	It allows the disclosure of data to public bodies if certain conditions are satisfied and, in any case, when it is "necessary to avoid a serious danger and imminent to public safety, or for the preservation of life and of the physical safety of a third party" (art. 13.3.)
Art. 10, processing of special categories of data Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate	**Art. 7 d.lgs. 15/2018, processing of special categories of data** The processing of data referred to in Article 9 of the GDPR is authorised only if strictly necessary and assisted by appropriate safeguards for the rights and freedoms of the data subject **and specifically provided for by European Union law or by law or, in cases provided for by law,** by regulation, or, without prejudice to the safeguards for the rights and freedoms, if it is necessary to safeguard a vital interest of the data

safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject. See also Working Group 29, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) - wp258.	subject or another natural person or if it relates to data made manifestly public by the data subject**.** **Art. 24 d.lgs. 15/2018 (Prior consultation with the Data Protection Authority)** proscribes the mandatory preemptive consultation of the Italian DPA when the data processing involves biometric data (N.B. its application was suspended by the moratorium of law 205/2021) **Art. 6 d.P.R. (Data processing presenting specific risks)** Data processing involving databases containing biometric data should be conducted in pursuance with the DPA's guidelines and should be subject to a preemptive communication to the latter.

	Art. 11 c.2. d.P.R. (Limits to the collection of data) Proscribes that the processing of "sensitive" data, including biometric data, is permitted "when it is necessary for the requirements of an intelligence, security or judicial police investigation or the protection of order and security to supplement other personal data". N.B. change from "strictly necessary" (LED) to "necessary".
Article 18 (Rights of the data subject in criminal investigations and proceedings) Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.	**Art. 10, 11, 12 Rights of the data subject** **Art. 14 Limitation to the rights of the data subject**

Other relevant provisions:

Art. 37 d.lgs. 51/2018 (Control Authority)
Establishes the competence of the DPA to judge on the application of the d.lgs 51/2018 the Italia DPA, including to judge on complaints filed ex. art. 39-40 d.lgs. 51/2018 (see below) which can be presented by an NGO (c.2, e). The Italian DPA is not competent to judge on data processing operations undertaken by "courts" (to be interpreted in a broad manner as including also public prosecutors) acting in their "judicial capacity". Moreover, it establishes (c.2, i) a general competence of the DPA to "monitor the technological and social developments that are of interest, if and insofar as they affect the protection of personal data, especially the evolution of information and communication technologies". The triggering of these functions/powers has little to no costs for data subjects.
Art. 39 (Complaint to the Data Protection Authority and judicial review) The complaints to the DPA are regulated by articles 142 and 143 of the Italian Data Protection Code.

Art. 40 Representation of data subjects
The data subject may grant power of attorney to a third sector entity subject to the discipline of Legislative Decree July 3, 2017, no. 117, which is active in the field of protection of the rights and freedoms of data subjects with regard to the protection of personal data, to exercise on its behalf the rights set forth in Article 39, without prejudice to the provisions on legal aid provided for in the Code of Civil Procedure.
Art. 47 Modes of processing and data flows by law enforcement agencies
The CED **ensures the periodic updating, proportionality, relevance, and non-exceedance of the personal data processed, including through authorized queries of the Criminal Records and Pending Charges Records** *(casellario giudiziale e del casellario dei carichi pendenti*) as set forth in Presidential Decree No. 313 of November 14, 2002, of the Ministry of Justice, or other databases of the Police Forces**,** which are necessary to pursue the purposes of art. 1, c.1.

5. Decisions, recommendations and reports of National Data Protection Authorities and other European/international privacy watchdogs or institutions

NDPAs, privacy watchdogs and institutions are of crucial importance in the protection of fundamental rights in terms of FRTs. They are independent public authorities that supervise and hold governments accountable by way of investigations, corrective powers and data protections law. They provide expert advice on data protection issues and handle complaints lodged against violations of the GDPR and relevant national laws. The DPAs discussed in this section are the only DPAs who have reacted on or assessed the subject in this research report in a relevant manner. In the following section decisions, recommendations and reports from various NDPAs and institutions will be discussed in terms of the use of FRT by law enforcement authorities and the circumstances in which the fundamental rights discussed above can be legally infringed upon.

5.1 The use of FRT by law enforcement authorities

Law enforcement use of FRTs poses a number of difficulties, chiefly because of the potentially catastrophic consequences of system errors or abuses in this area. The National Institute of Standards and Technology ("NIST") conducted research in 2019 that revealed that while some FR algorithms exhibited "undetectable" variations in accuracy across racial groupings, others indicated performance issues based on demographic factors including gender and race.[282] LEAs need to be aware of these potential performance issues and put in place the right governance procedures to address them.

[282] Patrick Grother, Mei Ngan, Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR, 2019. Available here.

Failure to implement such procedures could have grave repercussions. For instance, a false identification as a suspect in a theft investigation including FRT resulted in the arrest and detention of an innocent African American man in 2018 in the United States.[283] LEAs' use of FRTs can impair freedom of expression,[284] freedom of assembly and association,[285] and the right to privacy[286] in addition to rights like the presumption of innocence and the right to a fair trial[287] and due process.[288] Global policy activity has been more intense as a result of these concerns. Positions on this issue have been developed by significant US technology companies. Following a string of incidents in 2020, including the Clearview AI scandal,[289] which increased public mistrust of LEAs both in the US and abroad, IBM announced that it will no longer offer, develop, or research FRT, while Microsoft promised to halt selling FRT to US LEAs until federal regulation was put in place.[290] In 2022, Microsoft took things a step further by imposing new restrictions and controls on all FRT uses as a part of a larger framework of AI principles.[291] Amazon Web Services ("AWS") also extended its 2020 ban on police use of its recognition technology that it first imposed in 2021.[292] This mistrust and

[283] Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR, 2020. Available here.
[284] See para 3.3 for a discussion on the case law of the ECtHR regarding the right to freedom of expression and para 4.2 for the CJEU.
[285] Ibid.
[286] See para 3.2 for a discussion on the case law of the ECtHR regarding the right to privacy and para 4.1 for the CJEU.
[287] See para 3.1 for a discussion on the case law of the ECtHR regarding the right to a fair trial.
[288] Jay Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics and Privacy*, ACLU, 2019. Available here.
[289] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, The New York Times, 18 January 2020. Available here.
[290] Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress*, Vox, 11 June 2020. Available here.
[291] Sarah Bird, *Responsible AI Investments and Safeguards for Facial Recognition*, Microsoft, 21 June 2022. Available here.
[292] Amazon, *We Are Implementing a One-Year Moratorium on Police Use of Recognition*, 10 June 2020. Available here.

string of repercussions for the use of FRTs by LEAs in the US could act as a clear warning for Italian authorities regarding their lack of adequate regulation as discussed in the paragraphs above.

The policy agenda on FRT is now also being significantly shaped by courts. Brazil's Sao Paulo Court of Justice barred the implementation of FRT in the public transportation system in 2021.[293] Civil rights organisations that oppose the expanding use of FRT by public bodies saw this as a significant triumph. In a comparable case in the UK, the Court of Appeal determined that the South Wales Police's use of automated FRT at specific events and public locations was unlawful because it did not sufficiently define who could be on a watch list and where it could be used, it did have a legal basis for use in Common Law.[294]

Governments in certain countries have chosen to be cautious. In the Netherlands, that has been the situation.In a letter to lawmakers in 2019, the Minister of Justice and Security informed them of the current uses of FRT by law enforcement organisations and reiterated his support for effective governance procedures in relation to this sensitive technology as it poses a risk to fundamental rights such as Article 8 of the ECHR[295] and Article 17 of the International Covenant on Civil Rights and Politics ("ICCPR").[296] In addition, he contended that the current legislative framework and protections, both organisational and technical, are strong enough to guarantee that law enforcement authorities will use FRT

[293] Accessnow, *Privacy Win for 350,000 People in São Paulo: Court Blocks Facial Recognition Cameras in Metro*, 12 May 2021. Available here.
[294] Royal Court of Justice, *In the Court of Appeal (Civil Division) on Appeal from the High Court of Justice of Queen's Bench Division (Administrative Court)*, Case No. C1/2019/2670. Available here.
[295] As discussed at para 3.2.
[296] Rijksoverheid, *Letter of the Minister of Justice and Security of the Netherlands to MPs to Inform Them About the Use of Facial Recognition Technology by Law Enforcement Agencies (in Dutch)*, 20 November 2019. Available here.

responsibly. But before approving any more FRT usage or pilots, he demanded more privacy, ethical, and human rights impact evaluations.

5.1.1 The EU efforts

In order to avoid any mistakes that could lead, inter alia, to the unlawful use of evidence in a criminal trial obtained by way of FRTs, and therefore the infringement of the right to due process (amongst others), policymakers are working to restrict how and when LAEs use FRTs. Such is the course that the European Commission has advocated, having published its draft of an Artificial Intelligence Act in 2021 ("AI Act") which is a proposal for the regulation of AI in the EU.[297]

This comprehensive regulatory plan categorises AI applications into four distinct risk categories that are each subject to a set of rules.[298] On 11 May 2023, the Internal Market Committee and the Civil Liberties Committee approved an amended draft regulation.[299] The compromise text will be voted by the entire European Parliament during the 12-15 June session.

Provisions regarding remote biometric systems, such as FRTs, are included in this proposal. The most recent amendments to the AI Act modified extensively the list of prohibited artificial intelligence practices contained in Art. 5 of the proposal. Said article now bans the use of 'real-time' remote biometric identification systems in publicly accessible spaces.[300] The amendment also adds letter (e) to article 5,

[297] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD).

[298] Jorge Liboreiro, *'The Higher the Risk, the Stricter the Rule': Brussels' New Draft Rules on Artificial Intelligence*, Euronews, 21 April, 2021. Available here.

[299] European Parliament, *Draft Compromise Amendments on the Draft Report,* 11 May 2023. Available here.

[300] The previous version of the article included an extensive exclusion from such a prohibition for purposes of law enforcement which included: (i) the targeted search for specific potential victims of crime, including missing children; (ii)the prevention of a specific, substantial and imminent threat

prohibiting "the putting into service or use of AI systems for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, *unless they are subject to a pre-judicial authorisation* in accordance with Union law and *strictly necessary for the targeted search connected to a specific serious criminal offense* as defined in Article 83(1) of TFEU *that already took place for the purpose of law enforcement"*.

A similar strategy is emerging at the UN level, where the Office of the High Commissioner for Human Rights ("OHCHR") presented a report[301] on the right to privacy in the digital age to the Human Rights Council in 2021. In this report, the OHCHR urges the prohibition of AI applications that cannot be used in accordance with international human rights law. The report stated that remote biometric recognition significantly increases the ability of State authorities to systematically identify and track individuals in public spaces, undermining people's ability to go about their lives unobserved and having a direct negative impact on the exercise of the rights to freedom of expression, to peaceful assembly, and association as discussed above in relation to the ECtHR and CJEU. This is particularly true with regard to the use of FRT by LEAs in criminal proceedings. The report reiterates recommendations for a ban on FRT in public areas, at least until officials can show that there are no substantial problems with accuracy or disparate effects and that these AI systems adhere to strict privacy and data protection rules.

In parallel with the process of adopting the AI Act, the approval process is continuing for the Proposal for a Regulation of the European Parliament and of the

to the life or physical safety of natural persons or of a terrorist attack; (iii)the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

[301] United Nations, *Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet*, 15 September 2021. Available here.

Council on automated data exchange for police cooperation ("Prüm II"), submitted on 8 of December 2021.[302]

The future Regulation is expected to amend the existing framework on data exchange for law enforcement cooperation[303] in order to facilitate the exchange of information for the purpose of the prevention, detection and investigation of criminal and terrorist offences between Member States' law enforcement authorities, but also with Europol as the EU criminal information hub.

Related to this research, among the main innovations of Prüm II one can mention the inclusion of facial images as a new category of data to automated exchange (arts. 21-24) and the creation of a central router to which the national databases are connected. This router would serve as message broker, so that LEAs of the Member State could request a query by submitting biometric data to the router and this would dispatch the request for a query to the Member States' databases and Europol data simultaneously, ranking the replies resulting from the search (art. 37).

In this way, the exchange of new categories of data would not require new storage space, as the data would already be stored in the databases of the Member States according to national law, and the new data processing would be limited to the extent necessary to achieve its purpose and would only allow for the comparison of data on a case-by-case basis.

Despite the safeguards surrounding the processing of data such as their justification, quality check, and the keeping of logs, many doubts remain about

[302] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM/2021/784 final. Available here.
[303] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA, based on the 2005 Prüm Convention and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

what has been described by Ella Jakubowska, policy adviser at the civil rights NGO European Digital Rights (EDRi), as "the most extensive biometric surveillance infrastructure the world has ever seen".[304]

Some critical issues were highlighted in both Opinion 4/2022 of the EDPS[305] and the position paper by the EDRi network.[306]

In particular, on the one hand, EDPS points out many critical issues, including: the lack of a list of types of crimes which may justify the query, so the automated search of face images enabled by the Prum II framework could also be carried out for prevention, detection and investigation of any crime, even minor ones; the need to clarify the personal and the material scope of the measures, i.e. the categories of data subjects who will be directly affected; the requirement of additional safeguards to comply with the principles of necessity and proportionality.

On the other hand, the position paper EDRi emphasises how the proposal for Prüm II risks missing a vital opportunity to fix systemic issues in the exchange of data across borders by LEAs under the existing Prüm framework and calls on the EU's co-legislators to:

1. Implement specific rules for Member States' police databases prior to their connection to the Prüm II system, to ensure a high level of protection of fundamental rights (Section 1);
2. Remove the sharing of Europol-held third-country biometric data and remove Europol's own-initiative biometric searches, which lack a legal basis (Section 1);

[304] Her words are reported by Matt Burgess, "Europe Is Building a Huge International Facial Recognition System", Wired, 06 April 2022. Available here.
[305] EDPS, Opinion on the Commission's Proposal for the Regulation on automated data exchange for police cooperation ("Prüm II"), 4/2022. Available here.
[306] Available here.

3. Add additional safeguards to the sharing of reference data, as well as more broadly throughout the Prüm system in order to align to the LED (Sections 1 and 3);
4. Request a thorough necessity and proportionality assessment of the proposal for Prüm II, including requiring evidence and statistics to clarify whether the current framework is effective. If not, the co-legislators should delete all elements of the proposal that are not demonstrably necessary and proportionate (Sections 2, 4 and 5);
4. Delete the large-scale automated exchange of unidentified DNA data (Section 3);
5. Ensure all searches can only be undertaken on the basis of genuinely individual cases, and only in the event of serious crimes, with additional safeguards (Section 3);
6. Grant member states a meaningful right of refusal before the exchange of personal data (Section 3);
7. Fully reject the inclusion of facial image exchange in Prüm II due to the serious risks of fundamental rights violations (Section 4);
8. Limit the definition of police records to ensure that biased assumptions, hear-say and other illegitimate records will not be shared via Prüm II (Section 4);
9. Resist the attempt to add national driving license systems, which would treat whole populations as if they are suspected of serious crimes (Section 4).

As currently formulated, in fact, the text of the draft regulation on Prüm II risks weakening the scope of the AI Act, especially with regard to the human centric approach that emphasises the protection of fundamental rights, thus re-emerging risks of a generalised and indiscriminate use of facial recognition technologies by LEAs.

5.2 Justification for the interference with fundamental rights by the use of FRTs by law enforcement authorities

A substantial amount of personal data, including specific categories of data, must be processed to deploy FR systems. A person's identity is inextricably and permanently tied to their face and, more broadly, to their biometric information. As a result, the use of FR may infringe on several fundamental freedoms and rights protected by the EU Charter of Fundamental Rights, including those related to human dignity, freedom of movement, freedom of assembly, and others, in addition to privacy and data protection. As this research has shown this is especially important in the context of criminal justice and law enforcement.[307]

In principle, law enforcement should only use FRTs to handle biometric data for identifying purposes in a controlled or uncontrolled environment whilst the uncontrolled environment should be restricted, in general, to law enforcement purposes. “Uncontrolled” in this context would cover the cases in which biometric systems can only be used with the individual’s participation.[308] Only the security-related authorities with the necessary qualifications should carry it out. Depending on whether the goal is identification or verification, taking into account potential dangers to basic rights, and provided that the use of an individual's photos is the authorised collection, laws can establish alternative necessity and proportionality requirements. Both in setting up the database (watchlist) for identifying purposes and in deploying (live) FR technologies in an uncontrolled environment, stringent need and proportionality must be respected.[309] Live FR cameras are focused on a specific area and when individuals subsequently pass through that area their

[307] Ivi, 10.
[308] Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108, Guidelines on Facial Recognition, Council of Europe, 2021, 6. Available here.
[309] Ivi, 8.

images are streamed directly to a Live Facial Recognition system. This system contains a watchlist which is a list of persons wanted by the police and/or the courts, or those who pose a risk of harm to themselves or others.

When constructing databases or watchlists for specific, lawful, and explicit law enforcement reasons, laws should set forth certain guidelines and standards that law enforcement officials must follow (for example for individuals under suspicion of severe offences or who pose a risk to public security). As a result of the intrusive nature of these technologies, the law must ensure that law enforcement officials can prove the location and timing of the deployment of these technologies, justify the strict necessity and proportionality of the uses during the deployment phase of live FRTs in uncontrolled environments.[310]

In this section, the term "entities" covers data controllers,[311] and where applicable processors,[312] in the public sector including law enforcement and judicial authorities. When using live FR for surveillance, entities such as law enforcement and judicial authorities must make sure that the use of watch lists complies with data protection law and upholds the same standards of lawfulness, fairness, necessity, and proportionality. In cases where there is a collaboration with law enforcement, controllers must also make sure that roles and responsibilities (including controllership) are crystal clear and that the necessary governance and accountability measures are in place. The applicable specific legal requirements must be complied with by all parties.

Controllers must establish a legal basis for processing special category data such as biometric data as contained in article 9 of the GDPR and article 10 of the LED,

[310] Ivi, 9.
[311] According to article 4(7) of the GDPR, the data controller determines the purposes for which and the means by which personal data is processed.
[312] According to article 4(8) of the GDPR, the data processor processes personal data only on behalf of the controller.

and criminal offence data where necessary for processing to be legal. They must satisfy the prerequisites of those important legal entry points. Algorithms used in FRTs only ever offer *probabilities* that two faces belong to the same individual. There is therefore a certain margin of error in the context of use in the criminal trial for example, which causes people to be incorrectly flagged or identified.

The EDPB is aware of the necessity for LEAs to have access to the greatest resources so they can promptly find those responsible for terrorist attacks and other severe crimes. However, these instruments must be utilised strictly under the appropriate legislative framework and only in situations where they meet the necessity and proportionality requirements, as outlined in Article 52(1) of the EU Charter.

Under any circumstances, processing biometric data is a severe intrusion in and of itself. This is independent of the result, such as a successful match. Even if the biometric template is quickly removed following a no-hit match with a police database, the processing still counts as interference. Further risks associated with such processing include the possibility that the personal data obtained by the competent authorities would be misused due to unauthorised access to and use of the data, security breaches, etc. Risks frequently rely on the processing and its circumstances, such as the danger of unauthorised use or access by law enforcement or other parties. Nonetheless, some hazards are inherent given the distinctiveness of biometric data. A data subject cannot alter their distinctive features, such as the face or the iris, unlike an address or phone number. If biometric data were to be accidentally or unlawfully accessed, it may result in the data being compromised for use as passwords or cryptographic keys, or it could

be used for additional, unlawful surveillance operations to the disadvantage of the data subject.[313]

An act of law that either aims at or has the effect of restricting the relevant fundamental right may account for the interference with the data subject's fundamental rights.[314] It could also result from a private organisation that has been given legal authority to exercise public authority and public powers, or from a public authority acting with the same intent or consequence. The rights protected by Articles 7 and 8 of the EU Charter (as discussed at para 4.1) are directly interfered with by any legislative action that establishes a legal foundation for the processing of personal data.[315] The use of biometric data and FRT in particular in many situations also affects the right to human dignity, enshrined in Article 1 of the EU Charter. Human dignity requires that individuals are not treated as mere objects. FRT objectifies the face by calculating existential and highly personal traits, such as facial features, into a machine-readable form for use as a human licence plate or ID card. In the event that chilling effects are either intended by or result from the pertinent video surveillance of law enforcement authorities, such processing may also interfere with other fundamental rights, such as the rights under Articles 11, and 12 of the EU Charter as discussed at length above at para 4.2.[316]

There are several use cases for FRT that present unacceptable hazards to people and society (referred to as "red lines"). The EDPB and the European Data

[313] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 2022, cit., 12.
[314] Court of Justice of the European Union, C-219/91, *Johannes Stephanus Wilhelmus Ter Voort*, 28 October 1992, §36. Available here; Court of Justice of the European Union, C-200/96, *Metronome Musik GmbH v Music Point Hokamp GmbH*, 28 April 1998, §28. Available here.
[315] Court of Justice of the European Union, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, cit. §36; Court of Justice of the European Union, *Michael Schwarz contro Stadt Bochum*, cit. §23 and the following.
[316] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement,* cit., 259, 13.

Protection Supervisor ("EDPS") have demanded their universal prohibition due to these factors. Particularly, remote biometric identification of people in open areas presents a significant risk of privacy invasion and has no place in a democratic society because it requires extensive mass surveillance.

Additionally, the EDPB believes that AI-supported FR systems that group people based on their biometrics into groups based on their race, gender, or political or sexual orientation are incompatible with the Charter. The EDPB is also convinced that using FR or other comparable technology to infer a person's emotions is highly undesirable and should be banned, perhaps with a few properly justified exceptions. Furthermore, the EDPB contends that processing personal data in a law enforcement context that relies on a database populated by a mass-scale and indiscriminate collection of personal data, such as "scraping" facial images and photographs that are available online, particularly those made available via social networks, would not as a result meet the strict necessity requirement stipulated by Union law.[317]

Furthermore, the potential for bias and discrimination in AI systems such as FR is omnipresent. According to several technical studies[318] FR performs less precisely for specific demographic groups, such as women, members of underrepresented racial and ethnic groups, and perhaps those who are disabled.[319] Demographic factors like age, sex, race, and ethnicity can have a significant impact on the error

[317] European Data Protection Board, cit., 259, 10.

[318] See for example research from Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PMLR (2018), and studies from the U.S. Department of Commerce National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (December 2019) and Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification (August 2017)*; the EU FRA paper, Facial recognition technology: fundamental rights considerations in the context of law enforcement (November 2019); Disability, Bias, and AI, AI Now Institute NYU (November 2019).

[319] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Conference on Fairness, Accountability, and Transparency, 2018, 77-91. Available here.

rates in FRT. These problems might produce biassed or prejudiced results because they frequently result from design faults or poor training data. A watchlist's (often manual) compilation process, which forms the basis of an FR system, carries a risk of prejudice and discrimination as well. All these issues risk infringing the fairness principle within data protection law, as well as raising ethical concerns.

5.3 Key requirements and recommendations for controllers and law enforcement agencies according to international privacy institutions

5.3.1. The use of live facial recognition technology in public places" - ICO

Any use of personal information must be lawful, necessary, fair, and proportionate.[320] These are important criteria established under data protection law, as was already discussed above. Furthermore, additional safeguards are in place when there are greater threats to people's rights and liberties. The Information Commissioner Officer ("ICO") which is the national data protection authority in the United Kingdom, for example, emphasises that her office would base any investigation or regulatory evaluation on the facts of the case, taking into account the unique circumstances and pertinent regulations.[321]

Controllers must be open and transparent with individuals when determining if utilising FR is fair and must safeguard them from any unjustified negative effects. They should make sure that the algorithms guiding their systems generate results

[320] Article 5(1)(a) GDPR.
[321] Information Commissioner's Opinion, *The use of live facial recognition technology in public places*, Information Commissioner's Office, 2021, 51. Available here.

that are sufficiently accurate and take prejudice and discrimination into account. To employ live FRTs, controllers must be able to prove that it is reasonably necessary. To accomplish a particular goal, it should be a focused and efficient strategy. Controllers must show that they have thought about and excluded less intrusive choices for reasonable reasons. FR should not be used by controllers just because technology is available, increases productivity lowers costs or fits into a specific business model.[322]

Additionally, live FR use in public areas needs to be proportionate. Live FR systems that automatically and arbitrarily gather and analyse biometric data, possibly in bulk, without users' consent or control, could constitute a serious invasion of privacy. Controllers must explain how their strategy is justified by their desired goal. The dangers to people's interests, rights, and freedoms that might come from the project, for example the Italian moratorium which creates exceptions to the limitation of the use of biometric data by judicial authorities, must be evaluated as part of a DPIA. It's not simply about the potential harm that is immediate and visible. This includes the possibility of more subtle harm, such as social disadvantage, or the impossibility for people to exercise their right to data protection, other rights or to object to the use of their personal information.[323] Under the proposed moratorium for example, if biometric data obtained by way of FRTs is used as evidence in criminal proceedings, the accused will be deprived of exercising their right to data protection.

When procuring, purchasing, or designing any FR systems, controllers should take privacy and data protection into account. As should have been the case before the

[322] Directorate General of Human Rights and Rule of Law, *Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108 Guidelines on Facial Recognition*, Council of Europe, 2021, 11. Available here.
[323] ICO, cit., 265, 52.

multiple tenders launched by Italian authorities to enhance the SARIsystem or for the acquisition of new FR systems by the *Arma dei Carabinieri* as discussed above under para. 2.2. They should have made sure, for example, that the live FR services they purchase from suppliers have the necessary privacy and data protection safeguards built into the design. As mentioned above, in the case of Italy's *Arma dei Carabinieri,* no other documents could be found in terms of the tender, therefore no technical details or requirements are confirmed to have been met during these tenders. The law holds controllers, not technology vendors, accountable for this. The controller shall adhere to the data protection principles and permit persons to exercise their data protection rights if they determine that the processing can be justified. High levels of governance, including clearly defined operating procedures and continuing review mechanisms, are expected, according to the commissioner. Any related processing, including creating and keeping track of watchlists, must also adhere to data protection laws.[324]

5.3.2 "A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations"- UNICRI

The World Economic Forum, the International Criminal Police Organization ("INTERPOL"), the United Nations Interregional Crime and Justice Research Institute ("UNICRI") and the Netherlands Police have developed a global- and multistakeholder set of principles for the responsible use of FRT for law enforcement investigations.[325] In order to guarantee that law enforcement organisations use FRT appropriately, the following principles that will be discussed are considered by the UNICRI to be fundamental.

[324] Ivi, 53.

[325] United Nations Interregional Crime and Justice Research Institute, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, Insight Report, 2022. Available here.

In order to facilitate the identification of criminals/fugitives, missing persons, persons of interest, and victims, FRT must only be utilised as a legitimate investigative lead. The rights outlined in the so-called International Bill of Human Rights (which include, among others, the International Covenant on Civil and Political Rights, or ICCPR) and other pertinent human rights treaties and laws should always be upheld, especially the rights to human dignity, equality, and non-discrimination, the right to privacy, the right to free speech, association, and peaceful assembly, the rights of children and older people, persons with disabilities, migrants, and indigenous peoples, as well as the rights of migrants. Law enforcement should respect these rights and only employ FRT when it is necessary and appropriate to accomplish legal policing objectives. In international human rights law, any limitations or restrictions on human rights are only allowed if they are both necessary and reasonable to achieve a legitimate policing goal and are not implemented arbitrarily. These limitations must be set down in law and should be in line with the least invasive strategy for achieving this goal.[326]

The course of action to use FRT should always be made with the notion of striking a fair balance between allowing LEAs to use the latest technologies, which have been shown to be precise and secure, to protect people and society from security threats, and the requirement to protect individual human rights. LEAs thinking about using FRT should always give a documented and reasoned explanation for why FRT was selected and not other choices. From the first request to the utilisation of the search's findings, LEAs should always aim for and confine their use of FRT to a single, clearly defined objective that is inescapably connected to their investigative objectives.[327]

Lines of accountability for the results of a particular use of FRT must be well-defined and transparent. No analysis or results from FRT should ever be released

[326] Ivi, 20.
[327] Ivi, 21.

by a law enforcement agency without interpretation by an examiner and supervision by a manager with the necessary experience. As was discussed above, Italian authorities, for example, when utilising the AFIS-SSA database and using it separately applied in the use of the SARI-Enterprise, did not seek out or implement any independent oversight of the systems. FRT should only ever be used by trained professionals.

In order to evaluate the effectiveness of their algorithms during the design and deployment phases, vendors should be required by LEAs to adhere to FRT standards, such as those established by the International Organization for Standardization[328] ("ISO") and the European Committee for Standardization[329] ("CEN"). Using a transparent standardisation process, law enforcement organisations should require vendors to adhere to the aforementioned requirements and submit their algorithms for extensive independent audits and testing against the necessary test standards (lab tests and, if feasible, field tests). Agencies should choose the vendor who can exhibit the best-performing algorithm after reviewing each candidate. It is important to take every precaution to reduce the likelihood of prejudice and inaccuracy on the part of both humans and technology. Ex-ante and ex-post evaluation strategies should be used for this.[330] If not, as is the case in Italy as mentioned above, its application stands in clear contrast with the principles enshrined in the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, especially that of transparency.

[328] 'ISO/IEC TR 29794-5:2010', April 2010, available here.
[329] 'CEN/TS 17631:2021', n.d., available here.
[330] Ivi, 22.

The processing of probe images and reference databases by LEAs should be done in accordance with international, regional, and national laws and/or policies, and should include storage criteria, purpose limitations, retention periods, deletion procedures, etc. The gathering of probing image data ought to be done legally and with a defined goal in mind.[331] Otherwise, as was the case in Italy as discussed above, a DPA can find that the deployment of FRT can lack a legal basis to legitimise the automated processing of biometric data for FR in security applications. An appropriate legal basis should take account of all the rights and freedoms at issue and refer to the specific situations where such systems may be deployed – without leaving a wide margin of manoeuvre to the users of those systems.[332] To reduce the danger of mistakes, law enforcement authorities should set standards and thresholds for the picture quality of reference database images. Images from reference databases that fall short of the established criteria for image quality ought to be avoided.[333] The most recent findings in machine learning and remote biometrics research should be made available to or facilitated by law enforcement entities who use or intend to use FRT.

Finally, the public should have access to information about how law enforcement authorities employ FRT. The necessary official authorities, whether they be the law enforcement agency themselves or another government body, should convey this information and make it available permanently or upon request.

5.3.3 The *Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology* - Global Privacy Assembly

[331] Ivi, 23.
[332] European Data Protection Board, *Facial recognition: Italian SA fines Clearview AI EUR 20 million,* DPA Report, 2022. Available here.
[333] Ivi 24.

The International Conference of Data Protection and Privacy Commissioners, the predecessor to the Global Privacy Assembly (”GPA”), convened in 1979. For more than 40 years, the Assembly has served as the principal international venue for data protection and privacy authorities. The Assembly aims to take the lead on data protection and privacy issues on a global scale. More than 130 data protection and privacy authorities from around the world collaborate to do this.

The GPA also resolved to create a set of accepted principles and guidelines for the responsible use of individual data in FRT by law enforcement authorities, together with suggestions for risk mitigation. The Resolution recognised that potential uses of FRT might boost security and public safety, but it also made clear that these uses could also enable arbitrary or illegal surveillance, be extremely intrusive, yield biassed results, and compromise data privacy and human rights.

Authorities, businesses, and members of civil society have raised concerns over the privacy, legal, and ethical issues that FRT raises. The GPA has previously recognised the need to strive toward global legislation, standards, and models for issues that have a substantial impact on privacy. More effective prevention, detection, and rehabilitation of data protection and privacy issues are made possible thanks to this, and it also assures uniformity and clarity in the system of oversight for the digital economy. These guidelines apply to all forms and applications of FR used by law enforcement. Law enforcement authorities wishing to employ FRT must be aware of the relevant legal restrictions in their country of operation.[334]

Law enforcement authorities should have a clear legal basis for collecting and using biometric data. They should keep records of their legal usage of biometrics

[334] Global Privacy Assembly, *Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology*, 2022, 7. Available here.

for FR and be ready to present such records upon request. This covers the legal justification for both the creation of a biometric probe using an individual's image and the creation, access, or modification of any reference database that is being used or will be utilised. Authorities should be aware that implied consent generally shouldn't be relied upon for the gathering of sensitive personal information and that it frequently does not meet the requirement for consent in many jurisdictions.[335]

According to the GPA, authorities should establish, and be able to demonstrate, the reasonableness, necessity and proportionality of their use of FRT. Given the sensitivity of the information involved, the threshold for establishing necessity is high. It needs to be proven that the intended purpose is obvious and that FRT can accomplish this purpose, and that the purpose cannot reasonably be accomplished by less invasive means. It is not advisable to rely on convenience or desire to prove the necessity.[336] Authorities should review and safeguard against arbitrary or unlawful interference with privacy and other human rights in particular. They should generally anticipate that the use of FRTs may impinge unreasonably on people's rights to privacy and data protection. When deploying these technologies in an area that is open to the public, this interference is typically at its highest level.

It is imperative for authorities to conduct adequate impact assessments when evaluating potential effects on data protection and privacy rights (such as a Privacy Impact Assessment, DPIA or Human Rights Impact Assessment). They should be open with all those who could be impacted by how they are assessing and reducing privacy risks. They must take into account demographic differences (i.e. bias) in the system's operation (such as important performance gaps between groups) and application (e.g. differences in how the deployment of the system will impact individuals or groups). The usage of the FR system may have various effects on

[335] Ivi, 9.
[336] Global Privacy Assembly, cit., 314, 9.

different groups, and organisations should take this into account.[337] Regardless of the usage of FRT in publicly accessible locations, consider the potential "chilling effect" on rights like freedom of expression and freedom of association as well as the possibility of discrimination.[338] Consulting with representatives of marginalised groups to discuss the predicted effects and mitigation measures if the use of a system may have a disproportionately negative impact on those groups is of crucial importance.

The use of FR should include clear and effective accountability mechanisms. For all applications of facial recognition, authorities should establish precise governance and risk mitigation rules. The governance and risk management policies for FR should be established and maintained by organisations, together with a system for monitoring non-compliance (even from internal actors) and enforcing sanctions. The limitations and potential biases of FR systems, how to conduct facial comparisons, and ways to mitigate known risks like automation bias should all be covered in regular training for all users of facial recognition systems. All privacy rules should be followed when using FR. All data protection principles must be taken into account at all stages of an FR system's life cycle. Authorities should use a privacy-by-design methodology when creating facial recognition systems to guarantee that security measures are included from the start.[339]

5.4 Key data protection issues identified with the use of FRT by law enforcement authorities

[337] Ivi, 11.
[338] See para 3.3 for a detailed discussion on the relation between articles 10 and 11 of the ECHR and the possible “chilling effect”.
[339] Global Privacy Assembly, cit., 275, 14.

The first issue is the rapid and extensive automatic collecting of biometric data without clear justification. The ICO studied numerous cases of the use of FR in public spaces in the UK[340] and found that, for example, controllers more often than not inadequately explain why the automatic, indiscriminate processing of biometric data was required and appropriate.[341] There were no notable instances of data protection being implemented by design and default. The efficiency of FR in attaining the controller's goal against the potential effects on data subjects was not given any thought in the DPIAs studied by the ICO.

The lack of control for individuals and communities became clear from the research undertaken by the ICO. In most of the examples studied on how the UK GDPR and Part 2 of the Data Protection Act of 2018 apply to the use of FR in public settings, FR was used in public areas where the public's biometric data was being collected without their consent or knowledge. This is not to suggest that such processing must be based on consent, but controllers must provide a justification for processing biometric data in the absence of the subject's active participation. In light of this lack of participation, controllers must make sure that processing is fair, necessary, proportionate and transparent.

There is also a grave lack of transparency. In all of the ICO investigations, for example, into the usage of FR in public settings, transparency has been a major concern.[342] Transparency measures have frequently fallen short when it comes to the information provided in privacy statements, public communications, and visual signage. Data subjects may not have always understood when and when FR is used, how and why their data is processed, or how to exercise their rights.

[340] The Opinion studied for the purpose of this research focuses on how the UK GDPR and Part 2 of the DPA 2018 apply to the usage of live facial recognition in public settings. Except for competent authorities processing for law enforcement reasons, the intelligence services, or their processors, this regulation applies to any organisation employing live facial recognition.
[341] ICO, cit., 265, 19.
[342] Ivi, 20.

Transparency information was occasionally not given at all. The capacity of a person to exercise their data protection rights, such as the right of access, the right of erasure, and the right to object, may also be impacted by a lack of transparency.

Furthermore, the potential for bias and discrimination in AI systems such as FR is omnipresent. According to several technical studies[343] FR performs less precisely for specific demographic groups, such as women, members of underrepresented racial and ethnic groups, and perhaps those who are disabled.[344] Demographic factors like age, sex, race, and ethnicity can have a significant impact on the error rates in FRT. These problems might produce biassed or prejudiced results because they frequently result from design faults or poor training data. A watchlist's (often manual) compilation process, which forms the basis of an FR system, carries a risk of prejudice and discrimination as well. All these issues risk infringing the fairness principle within data protection law, as well as raising ethical concerns.

There are numerous issues with watchlist governance. It is unclear from the examples researched by the ICO in their Opinion whether watch lists were always created and maintained in a legitimate, impartial, and open manner. Concerning watch lists, data subjects must be able to exercise their rights. These include the freedom to information, correction, erasure, and objection. These rights also cover any watch list information that is shared with third parties as well as any other FR records that controllers may possess. One must question the proportionality and

[343] See for example research from Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, cit., and studies from the U.S. Department of Commerce National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (December 2019) and Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification (August 2017)*; the EU FRA paper, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* cit.; Disability, Bias, and AI, AI Now Institute NYU (November 2019).

[344] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Conference on Fairness, Accountability, and Transparency, cit., 77-91

necessity of some watchlist data sharing between organisations. Any usage of exemptions from the GDPR (such as the right to information for data subjects) requires a convincing justification.[345]

5.5 Lack of due diligence concerning software

In the ICO's work reviewing DPIAs, they identified a lack of due diligence on the part of controllers in respect of the technology they purchase from manufacturers. Some have given the technical effectiveness of the systems they want to deploy a cursory examination. The ICO maintains that in some instances, controllers have not done enough to carefully consider the accuracy claims made by manufacturers for their systems, presenting accuracy rates without a clear knowledge of their origin or relevance to the controller's planned use case.

Public authorities typically rely on private companies for procuring and deploying FRT. The development of technical solutions that support respect for fundamental rights, particularly the security of personal data, can be greatly aided by industry and the scientific community. But to achieve this, technical requirements and agreements must take into account fundamental rights. The EU Public Procurement Directive (2014/24/EU) made EU Member States' commitment to ethical public procurement when making purchases of goods or services stronger. The data quality used to develop the programme and the data quality utilised when it is deployed have a significant impact on the accuracy of FRT. Authorities must utilise the information that is correct and current under the concept of data accuracy, which is expressed in Article 5 (1) (d) of the GDPR and Article 4 (1) (d) of the LED.[346]

[345] ICO, cit., 265, 20 - 21.
[346] Analysed above at para 4.7.

The biometric templates and digital images used during law enforcement activities must be correct and up-to-date, according to NDPAs and other privacy watchdogs, as discussed above. For instance, to avoid potential false matches, the quality of the biometric templates and photographs entered into watchlists by law enforcement authorities must be examined since poor-quality images might increase the frequency of errors. The sources of the photographs included in the watchlist, which demand strict adherence to data privacy rules including the principle of purpose limitation, are closely related to this. In the event of erroneous matches, the entities will make all practical efforts to prevent similar incidents in the future and guarantee the precision of digital photographs and biometric templates.[347]

Due diligence regarding system performance should be made with reference to extensive independent testing like those carried out by NIST in the US. These evaluations offer a transparent, reliable scientific performance baseline. The objectives and conditions of the real-world applications of the FRT (including the data landscape, the operators of the technology, timetables affecting decision-making using the technology, etc.) should be modelled as closely as possible in independent lab tests to validate the performance of the FRT.

In order to get the system evaluated, LEAs should alert the technology vendor to any pertinent problems found. LEAs should prepare for, and set up procedures for, routine updates or replacements of the FRT in order to capitalise on accuracy advances.[348] This is the case in Italy as LEAs regularly issue tenders, as discussed above at 2.2.1. However, without prior oversight of the use of the system, the criminalization of foreign nationals has been deeply established in Italian

[347] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 9
[348] UNICRI, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, Insight Report, cit., 22

technological infrastructure without any recourse or regulation. Without proper oversight of the use of this system, there is a concrete risk of producing false positives and violating the rights of certain categories of particularly vulnerable people.[349]

5.6 Pervasive danger of potential false positives

FR systems' technical efficiency and statistical precision are particularly challenging as well. The ICO has identified specific data protection risks which can be raised by AI systems such as FR. One of these is statistical accuracy. FR systems may produce "false positives" or "false negatives" if their statistical precision is insufficient. In some circumstances, false results could have inconsequential repercussions. Others might result in interventions like increased surveillance, ejection from the area, or even being reported to law enforcement and perhaps detained. High numbers of incorrect results would raise concerns about the necessity and fairness of the FR system.

The new focus on FRT is a result of the significant accuracy improvements made since 2014. Increased processing capacity, vast amounts of data (digital photographs of people and their faces), and the application of contemporary machine learning algorithms are mostly responsible for the accuracy improvements. There are many various ways to evaluate and assess accuracy, depending on the task, purpose, and context of its use. This makes determining the necessary level of accuracy for facial recognition software problematic. When using the technology in locations with high foot traffic, like railway stations or

[349] Hermes Center for Transparency and Digital Human Rights, cit., 34.

airports, a relatively tiny percentage of errors (around 0.01%) still result in hundreds of people being detected incorrectly.[350]

Additionally, some groups of people may have a higher likelihood of being mismatched than others. Error rates can be calculated and interpreted in a variety of ways, therefore care must be taken. Questions about how readily a system can be fooled by, for example, phoney facial photos are crucial in terms of accuracy and errors as well, especially for law enforcement purposes. Similar to other machine-learning algorithms, facial recognition technologies have binary outcomes, which means that there are only two possible results. False positive and false negative results are related to both the accuracy of data processing and the quality of the data. To ensure accurate processing, addressing this necessitates routine correction and updating of the facial photos saved in a watch list.

[350] EUAFR, cit., 287, 9.

6. Conclusions

Let us draw some conclusive remarks, which will guide the next phase of this research. The conclusions will follow the structure of the research.

Chapter 2 - SARI, the moratorium and the Italian regulation on the principle of fair trial

Upon the commencement of this research, we hypothesised the possibility of raising a question of 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.

This affirmation leads us to an important reflection: **what is going to happen when the moratorium will cease to have effect on December 31, 2023?** Indeed, it is unlikely that the Italian Parliament will adopt specific regulation before then. The most probable outcome is a re-expansion of the regulation applicable before the enactment of the moratorium. It follows that **public authorities** or private entities **will be allowed to install and use video surveillance systems with FR systems** operating through the use of biometric data **in public places or places open to the public**, provided that they obtain authorization from the Italian DPA. In other words, there might be a lot more cases like the ones in Como and Torino. It would be interesting to analyse which legal provisions would be used by municipalities to justify this data processing, provided that the DPA has deemed art. 6, c. 6 Decree-law 11/2009 inadequate. It is for this reason that StraLi, through

the support of external researchers, has been sending municipalities and police headquarters questionnaires to collect data on the matter. The results of the research will be the object of analysis in the next phase.

Certainly, when it comes to the use of SARI (or other FR tools) by LEAs, bringing a claim to the DPA seems to be strategic for a number of reasons. First of all, the DPA is competent on the enforcement of the LED (according to art. 37 d.lgs. 51/2018). Its jurisdiction can be triggered via complaints ex. art. 39-40 d.lgs. 51/2018, which can also be filed by an NGO (c.2, e). Consequently, StraLi would be able to intervene directly on behalf of an individual. Moreover, the DPA also possesses a general competence to monitor the technological and social developments that are of interest, if and insofar as they affect the protection of personal data. As such, it could be possible to trigger an investigation on whether public authorities are respecting the contents of the LED. Furthermore, complaints to the DPA represent a cost-free litigation tool. Finally, it is argued here that it could be possible to bring a claim regarding the transparency and the composition of the AFIS-SSA database. Indeed, one could ask herself whether its current composition is compatible with art. 6 LED (art. 4 d.l.gs. 51/2018) which mandates that “Member States shall provide for the controller, where applicable and as far as possible, to **make a clear distinction between personal data of different categories of data subjects”**.

However, as mentioned above, the Italian DPA is not competent to judge on data processing operations undertaken by courts (to be interpreted in a broad manner as including also public prosecutors) acting in their “judicial capacity”. Moreover, DPAs only deal with data protection and privacy aspects, which are distinguished from aspects pertaining purely to criminal law guarantees for defendants and for the defence.

As a result, the only way to challenge the use of SARI by judicial authorities appears to be via the criminal trial and its rules. The use of SARI's output as evidence or as the underlying reason to request a restrictive measure of liberty would trigger the application of certain protections, enshrined in the principle of due process at both the national and European/international levels. Thus, it is necessary - and it is one of the purposes of this research - to search for a "pilot case", that is, a case in which outputs of SARI (or other systems) have indeed "entered" a criminal trial. Such an activity is proving difficult, especially because, as pointed out above, the cases which have attracted attention regard cases where the use of SARI-Enterprise lead to a correct assessment - not that this suspends the application of the principle of adversary proceedings, but it might hinder the outcome of a litigation action. Rather than a constitutional court judgement, it might be effective to obtain a ruling from the *Corte di Cassazione* on the legitimacy of treating FR-evidence as atypical evidence under Article 189 of the Code of Criminal Procedure.

In addition, a strategic solution appears to be an advocacy campaign aimed at improving a culture of transparency regarding the use and functioning of FR tools, as well as their explicit regulation. It is only by ensuring transparency that due process guarantees can be enacted fully.

These will be the insights on which the next phase of this research will be based.

Chapter 3 - The European Convention on Human Rights

Due to the potential opportunity to file a case before the European Court of Human Rights on the use of FRT by law enforcement and judicial authorities as currently regulated in the Italian legal framework, an analysis of the impacted human rights

safeguarded by the European Convention on Human Rights, as well as the Court's jurisprudence was crucial.

Article 6 ECHR protects the right to a fair trial and encloses all the above-mentioned principles and elements. 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". From the above stems that, by using FR tools to the purposes of prevention and suppression of criminal offences: 1) the defence would be placed at a disadvantage position compared to the prosecution as it is not (necessarily) aware of the design and functioning of the FRT used nor of the process that has been followed to obtain such outcome (i.e. evidence), therefore being in a situation of mis-balance of arms within the criminal proceedings. 2) While the ECtHR rarely finds a violation of Article 6 due to unlawfully obtained evidence (for example in breach of Article 8), it has developed through its case-law the so-called overall fairness test. Through this test, the Court of Strasbourg tries to assess whether the concerned (criminal) proceeding has been fair as a whole. Among the elements analysed, the ECtHR would determine whether the defence had challenged the evidence adduced by the prosecution to prove the guilt of the defendant. However, challenging the evidence which is the result of the use of FRT becomes more complicated for the defence due to the opacity of the tool and of the process followed to obtain the outcome. In addition, even trying to acquire this information through an external consultant would put the defence in a disadvantage position, not only because few experts on the matter exist in Italy, but above all because this might not be in the financial capacity of every defendant - this would lead to an indirect and unjustified discrimination of the criminal justice system. 3) The above would lead the defence to need to demonstrate (without the actual

possibilities to do so) that the concerned defendant is not guilty for the charged offence, which would be an arbitrary reversal of the burden of proof, as well as an unlawful violation of the presumption of innocence which should guide every criminal process in Italy. From the above stems that the existing Italian regulation on FRT would have great impact on the right to fair trial and due process guarantees as safeguarded by Article 6 ECHR and interpreted by the Court of Strasbourg.

Article 8 safeguarded the right to a private life, declined as the right to privacy. While the European Convention on Human Rights admits derogation to such right, it also foresees criteria (ex Article 8 (2)) to be met in order for the derogation to be considered lawful. Through its case-law, the ECtHR has developed the so-called three-part test. The derogation needs to: 1) pursue one of the legitimate aims listed by the relevant norm (in which national security, public safety as well as the prevention of disorder or crime are mentioned); 2) be a necessary and proportional measure in comparison to the goal pursued, meaning that the it cannot be disproportionately intrusive to the concerned right; and 3) be in accordance with the law, namely the legal basis that allow the derogation of the right to privacy should be clearly foreseen in the national legislation. As extensively see above, SARI Real-Time was considered by the Italian DPA to lack of the sufficient legal basis, and, therefore, we would assume this would also be the approach of the Court of Strasbourg should the Italian legislation remain the same (and the moratorium not renewed as the law enforcement authorities are concerned).

The next step of the research would try to understand whether a submission to the ECtHR can be the most strategic path to follow in order to challenge the Italian legislation at stake - should both the procedural and substantial elements exist.

Chapter 4 - The Charter of Fundamental Rights of the European Union and Regulation 679/2016 (GDPR)

Similar conclusions can be achieved by reference to the jurisprudence of the European Court of Justice. Judgments on the use of FRTs were found only with reference to some of the analysed articles, in particular with regards to Articles 8 (protection of personal data) and 47 (right to an effective remedy).

In the decisions found, however, the CJUE established proportionality between the use of FRTs and the fundamental rights sacrificed, deeming the general or special prevention objective pursued to be preponderant. In particular, the limitations to the rights under scrutiny were deemed justified to ensure, for instance, national security or to combat terrorism. Also with regard to the GDPR, the CJEU took a residual position with regard to the balance between freedom of expression and data protection, merely providing a limited set of elements useful to verify whether the activity of data disclosure could fall within the notion of 'journalistic purposes' and thus constitute an exception to the protection of personal data. Conversely, the impact of FRTs on the freedoms of expression and association protected by Article 11 of the Charter, on the right to non-discrimination enshrined in Article 21, on the right to access personal data, i.e. the right to good administration under Article 41 of the Charter was not directly assessed by the CJEU.

Chapter 5 - Decisions, recommendations and reports of National Data Protection Authorities and other European/international privacy watchdogs or institutions

Depending on the objective, setting, and extent of use, FRT has a variety of implications for fundamental rights. This is particularly relevant in the area of law enforcement and criminal justice. Several consequences for fundamental rights

are brought on by the technology's imprecision. Although accuracy has significantly improved, the technology still has a certain rate of error, which may have a negative effect on fundamental rights. However, even if there were no errors at all, a number of fundamental rights issues would still exist. Fundamental rights violations are difficult to forecast in light of the rapidly evolving technology. Therefore, **it is crucial that developments in FR are closely monitored by independent supervisory agencies**. Oversight authorities need sufficient authority, resources, and knowledge to prevent fundamental rights violations and effectively assist victims whose fundamental rights are compromised by FRT. FRT deployment and use must be governed by a clear and sufficiently comprehensive legislative framework, which should be modelled after the large-scale EU IT systems.

Bibliography

LEGISLATION, RECOMMENDATIONS, REPORTS, POLICY PAPERS

European Union

Council Decision 2008/615/JHA, of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

Council Decision 2008/616/JHA, of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

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

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

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 of such data

European Commission, Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 2021/0106 (COD)

European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and

Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM/2021/784 final. Available here

European Data Protection Board, F*acial recognition: Italian SA fines Clearview AI EUR 20 million,* DPA Report, 2022

European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 2022

European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices – version for public consultation*, Brussels, 10 July 2019

European Data Protection Supervisor, *Facial recognition: A solution in search of a problem?*, Wojciech Wiewiórowski European Data Protection Supervisor, 2019.

European Data Protection Supervisor, Opinion on the Commission's Proposal for the Regulation on automated data exchange for police cooperation ("Prüm II"), 4/2022. Available here

European Parliament, Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)).

European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019

European Union Agency for Fundamental Rights, *Getting The Future Right - Artificial Intelligence and Fundamental Rights*, 2020

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)

Regulation (EU) No 603/2013 of the European Parliament and of the Council, of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the

criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

Working Group 29, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) - wp258. Available here.

COUNCIL OF EUROPE

Convention for the protection of individuals with regard to the processing of personal data, 1981

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 128th Session of the Committee of Ministers, 2018

European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, December 2018

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data Convention 108, *Guidelines on Facial Recognition*, Council of Europe, 28 January 2021

Directorate General of Human Rights and Rule of Law, *Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108 Guidelines on Facial Recognition*, Council of Europe, 2021

Ad Hoc Committee on Artificial Intelligence and The Alan Turing Institute, "*Artificial Intelligence, Human Rights, Democracy, and the Rule of Law*", 2021

Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, Committee of experts on human

rights dimensions of automated data processing and different forms of artificial intelligence, 26 June 2019

Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights* – Recommendation, Council of Europe, Strasbourg, May 2019

EUROPEAN COURT OF HUMAN RIGHTS

Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb), Updated on 31 August 2021

Guide to the Case-Law of the European Court of Human Rights, Data protection, updated on 31 August 2021

Research Division, *Internet: case-law of the European Court of Human Rights*, 2015

UK surveillance regime: some aspects contrary to the Convention, Press Release issued by the Registrar of the Court, ECHR 165 (2021), 25 May 2021

ITALY

Decreto Ministro Interno 24 maggio 2017 recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'art. 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196

Law 1 April 1981, n. 121, nuovo ordinamento dell'Amministrazione della pubblica sicurezza

Law 23 December 1993, n. 547, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

Law 3 August 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto

Law 30 June 2009, n. 85, Adesione della Repubblica italiana al Trattato concluso il 27 maggio 2005 tra il Regno del Belgio, la Repubblica federale di Germania, il Regno di Spagna, la Repubblica francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria, relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale (Trattato di Prum). Istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA. Delega al Governo per l'istituzione dei ruoli tecnici del Corpo di polizia penitenziaria. Modifiche al codice di procedura penale in materia di accertamenti tecnici idonei ad incidere sulla libertà personale.

Law 3 July 2014, n. 99, Ratifica ed esecuzione dell'Accordo fra il Governo della Repubblica italiana e il Governo degli Stati Uniti d'America sul rafforzamento della cooperazione nella prevenzione e lotta alle forme gravi di criminalità

“T.U.L.P.S.” (regio decreto 18 giugno 1931, n. 77), Testo unico delle leggi di pubblica sicurezza

Regio decreto 6 maggio 1940, n. 635, Approvazione del regolamento per l'esecuzione del testo unico 18 giugno 1931-IX, n. 773 (TULPS), delle leggi di pubblica sicurezza

Decree law 21 March 1978, n. 59, converted into law, 18 May 1978, n. 191, Norme penali e processuali per la prevenzione e la repressione di gravi reati

Decree law 25 July 1998, n. 286,Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero

Law 3 December 2021, n. 205 (Conversion of decree law 8 October 2021, n. 139, recante disposizioni urgenti per l'accesso alle attivita' culturali, sportive e ricreative, nonche' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali

Law 1 April 1981, n. 121, Published in the Official Journal (*Gazzetta Ufficiale*) on 10 April 1981, n. 100, Nuovo ordinamento dell'Amministrazione della pubblica sicurezza

Legislative decree 18 May 2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

OTHER

United Nations Interregional Crime and Justice Research Institute, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, Insight Report, 2022

United Nations, *Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet*, 15 September 2021

CASE LAW

COURT OF JUSTICE OF THE EUROPEAN UNION

C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 3 May 2014

C-136/17, *GC and Others (De-referencing of sensitive data),* 24 September 2019

C-200/96, *Metronome Musik GmbH v Music Point Hokamp GmbH***,** 28 April 1998

C-205-21, *Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost*, 26 January 2023

C-219/91, *Johannes Stephanus Wilhelmus Ter Voort*, 28 October 1992

C-245/2020, X *and Z v Autoriteit Persoonsgegevens*, Judgment of the Court, First Chamber, 24 March 2022

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Opinion of Advocate General Kokott, 18 July 2007

C-305/05, *Ordre des barreaux francophones et germanophone and others v. Conseil des ministres*, 26 June 2007

C-356/12, *Wolfgang Glatzel v. Freistaat Bayern*, 22 May 2014

C-415/11, *Mohamed Aziz v. Caixa d´Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa)*, 14 March 2013

C-520/18, *Ordre des barreaux francophones et germanophone and Others*, 15 January 2020

C-54/96, *Dorsch Consult Ingenieurgesellschaft mbH c. Bundesbaugesellschaft Berlin mbH*, 17 September 1997

C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Other*s, 8 Aprile 2014

C-604/12, *H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General*, 8 May 2014

C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020

C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, 1 October 2019

C-131/15 P, *Club Hotel Loutraki*, 21 December 2016

C-291/12, M*. Schwarz v. City of Bochum*, 17 October 2013

C-300/11, *ZZ v Secretary of State for the Home Department*, 4 June 2013

C-418/11, *Texdata Software GmbH*, 26 September 2013

Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016

Joined cases C-482/13, C-484/13, C-485/13, C-487/13, *Unicaja Banco SA v. José Hidalgo Rueda and Others, Caixabank SA v. Manuel María Rueda Ledesma and Others, Caixabank SA v. José Labella Crespo and Others and Caixabank SA v. Alberto Galán Luna and Others*, 21 January 2015

Joined Cases C-511/18, *La Quadrature Du Net and Others* and *C-512/18 French Data Network and Others*, 6 October 2020

Joined Cases C-514/07 P, C-528/07, *Kingdom of Sweden v Association de la presse internationale ASBL (API) and European Commission (C-514/07 P), Association de la presse internationale ASBL (API) v European Commission (C-528/07 P) and European Commission v Association de la presse internationale ASBL (API) (C-532/07 P),* 21 September 2010

Joined Cases C-78-79/16, *Pesce and Serinelli*, 9 June 2016

Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert,* Opinion of Advocate General Sharpston, 17 June 2010

Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifer*, 9 November 2010

T-49/07, *Sofiane Fahas v. Council of the European Union*, 7 December 2010

EUROPEAN COURT OF HUMAN RIGHTS

Benghal v. the UK, Application No. 4755/16, 25 May 2019

Kennedy v. United Kingdom, Application No. 26839/05, 18 May 2010

Amann v. Switzerland, Application no. 27798/95, 16 February 2000

Brunet v. France, Application No. 21010/10, 18 September 2014

Centrum för Rättvisa v. Sweden, Application No. 35252/08, 19 June 2018

Dragoş Ioan Rusu v. Romania, Application No. 22767/08, 31 October 2017

Garcia Ruiz v. Spain (Grand Chamber), Application No. 30544/96, 21 January 1999

Gaughran v. the UK, Application No. 45245/15, 13 June 2022

LL v. France, Application no. 7508/02, 10 December 2006

Roman Zakharov v. Russia, Application no. 47143/06, 4 December 2015

S. and Marper v. United Kingdom, Applications Nos. 30562/04 and 30566/04, 4 December 2008

Schenk v. Switzerland, Application No. 10862/84, 12 July 1988

The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application. No. 62540/00, 2007

Uzun v. Germany, Application No. 35623/05, 2 September 2010

Weber and Saravia v. Germany, Application. No. 54934/00, 29 June 2006

NATIONAL DECISIONS

Cass., pen. Sez. Un., n. 26795.

Cass.pen., sez. V, n. 22612/2009

Cass. pen., sez II, n. 29847/2016

Cass. pen., sez. VI, n. 49758/2012

Cass. pen. sez. IV, n. 39731

Cass. pen. sez. I, n. 21823/2020

Cass. pen., Sez. IV, n. 43786/2010

R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341 (Admin)

Corte Cost., 25 ottobre 2000, n. 440

Italian Data Protection Authority, General Application Order Concerning Biometrics - 12 November 2014, n. 513.

CNIL, Facial recognition: 20 million euros penalty against CLEARVIEW AI, 2022

Swedish Authority for Privacy Protection, Police unlawfully used facial recognition app, 202

Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Clearview AI, provvedimento n. 50 del 10 febbraio 2022

Verwaltungsgericht Gelsenkirchen, 2018, 14 K 3543/18 (in German only)

Royal Court of Justice, *In the Court of Appeal (Civil Division) on Appeal from the High Court of Justice of Queen's Bench Division (Administrative Court)*, Case No. C1/2019/2670

ARTICLES, BOOKS & NEWSPAPER ARTICLES

Accessnow, *Privacy Win for 350,000 People in São Paulo: Court Blocks Facial Recognition Cameras in Metro*, 12 May 2021

Allyn B., *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR, 2020

Amazon, *We Are Implementing a One-Year Moratorium on Police Use of Recognition*, 2020.

Bampasika E., *Artificial Intelligence as Evidence in Criminal Trial*, 2020

Bartoli L., *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, La legislazione penale, 2022

Bigo D. - Carrera S. - Hernanz N. - Jeandesboz J. - Parkin J. - Ragazzi F. - Scherrer A., *Mass Surveillance on Personal Data by EU Member States and its Compatibility with EU Law*, CEPS Paper in Liberty and Security in Europe, N. 62, 2013

Bird S., *Responsible AI Investments and Safeguards for Facial Recognition*, Microsoft, 21 June 2022

Blackstone Chamber, *Big Brother Watch and Others v the United Kingdom*, 26 May 2021

Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Conference on Fairness, Accountability, and Transparency, 2018

Burgess M., "Europe Is Building a Huge International Facial Recognition System", Wired, 06 April 2022. Available here

Buzura A.M., N*uove forme di atipicità probatoria in materia di videoregistrazioni investigative*, Archivio Penale, 2022

Consulenza Legale Italia, *Precedenti di polizia e la cancellazione dal C.E.D – una guida rapida*

Carrer L. Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale, Wired, 9 June 2020

Currao E., *Facial recognition and fundamental rights: setting the balance,* Diritto penale e uomo, fascicolo 5/2021, Diritto penale e uomo, fascicolo 5/2021, Maggio 2021

Darin Goldberg R., *You Can See My Face, Why Can't I? Facial Recognition and Brady,* Columbia Human Rights Law Review, 2021. Available here

Dazzan A., "Udine, il comune stanzia 675mila euro per 67 videocamere a riconoscimento facciale. Ma non possono essere usate (per ora)", Il Fatto Quotidiano, 4 October 2021. Available here.

Della Torre J.*, Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, Diritto Penale Contemporaneo 1/2020

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg,* 2018.

Fair Trial, *Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe*", 2022

Fair Trial, *Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU*, 2022

Fair Trials, *Unlawful evidence in Europe's courts: principles, practice and remedies*, October 2021

Gialuz M., *Quando la Giustizia Penale Incontra L'Intelligenza Artificiale: Luci e Ombre dei Risk Assessment Tools tra Stati Uniti ed Europa*, Diritto Penale Contemporaneo, 2019

Gialuz M., Quattrocolo S., *AI and the administration of Justice in Italy,* e-Revue Internationale de Droit Pénal, 2023

Giuzzi C., Milano, stupro a Cascina Gobba: il selfie davanti al Duomo che ha incastrato il violentatore, Corriere della Sera Milano, 29 August 2021

Global Privacy Assembly, *Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology*, 2022

Grother P., Ngan M., Hanaoka K., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR, 2019

Heilweil R., *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress*, Vox, 11 June 2020

Hermes Center for Transparency and Digital Human Rights (Laura Carrer - Riccardo Coluccini) *Technologies for Border Surveillance and Control in Italy. Identification, Facial Recognition, and European Union Funding*, 2021

Hill K., *The Secretive Company That Might End Privacy as We Know It*, The New York Times, 18 January 2020

Information Commissioner's Opinion, *The use of live facial recognition technology in public places*, Information Commissioner's Office, 2021

Jackson K., *Challenging Facial Recognition Software in Criminal Cour*t, The Champion, 2019. Available here

Kellerbauer M., Klamert M. and Tomkin J.., *The EU Treaties and the Charter of Fundamental Rights*, Oxford University Press, 2019

Kokott J., Sobotta C., *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,* International Data Privacy Law, 2013, Vol. 3, No. 4

Laganà M., *Facial Recognition And Human Rights In Europe*, Human Rights Pulse, 1 April 2022

Liboreiro J., *'The Higher the Risk, the Stricter the Rule': Brussels' New Draft Rules on Artificial Intelligenc*e, Euronews, 21 April, 2021

Ligeti K. - Garamvölgyi B. - Ondrejová A. - von Galen M., *Admissibility of Evidence in Criminal Proceedings in the EU, The Future of EU Criminal Justice - Views from the Experts*, eucrim 3/2020

Lopez R., *La rappresentazione facciale tramite software*, in Le indagini atipiche, A. Scalfati (ed), Giappichelli, 2019

Massaro A., Giraldi A., Grossi L., Notaro L., Sorbello P., Università degli Studi "Roma Tre", *Intelligenza Artificiale e Giustizia Penale*, December 2020

McBride J., *Application of the European Convention on Human Rights and harmonisation of national legislation and judicial practice in line with European standards in Georgia*, European Union - Council of Europe joint project

Mobilio G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021

Quattrocolo S., *Intelligenza Artificiale e Giustizia: nella Cornice della Carta Etica Europea, gli Spunti per Un'Urgente Discussione tra Scienze Penali e Informatiche*, La Legislazione Penale, 18 December 2018

Rossi Da Pozzo F., *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, rivista Eurojus, 2018.

Sacchetto E., *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale,* Legislazione Penale, 2020

Sacchetto E., *Riconoscimento Facciale, l'approccio Italiano è in Antitesi Alla Ue: I Nodi,* Agenda Digitale (blog), 7 December 2022. Avaialble here

Saetta B., *Convenzione 108 del Consiglio d'Europa*, Protezione dati personali/ Data Protection, 2018

Saponaro L., L*e nuove frontiere tecnologiche dell'individuazione personale*, Archivio Penale n. 1/2022

Stanley J., *The Dawn of Robot Surveillance: AI, Video Analytics and Privacy*, ACLU, 2019

Torre M., N*uove tecnologie e trattamento dei dati personali nel processo penale,* Diritto penale e processo 8/2021

Tonacci F., Roma, il "cervellone" che ha scovato l'aggressore di Termini: meno di un minuto per cercare tra 10 milioni di volti, Repubblica, 5 January 2023

Valli R., *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, Il Penalista, 16 gennaio 2019

OTHER SOURCES

Polizia di stato, Avviso esplorativo, ex art. 66, comma 1, del d. lgs. n. 50/2016, finalizzato alla partecipazione ad una procedura negoziata senza previa pubblicazione del bando di gara per l'approvvigionamento di apparecchiature hardware e software finalizzate a potenziare le attuali funzionalità e prestazioni delle due componenti del sistema automatico riconoscimento immagini (SARI), denominate: SARI Enterprise e SARI real-time, in uso alla direzione centrale anticrimine nell'ambito del progetto "falco extended" (progetto n. 87.5.1) - fondo sicurezza interna 2014- 2020. Available here

Ministero dell'Interno, Esito di gara-Procedura negoziata senza previa pubblicazione del bando di gara per l'approvvigionamento di apparecchiature hardware e software finalizzate a potenziare le attuali funzionalità e prestazioni delle due componenti del Sistema Automatico Riconoscimento Immagini (SARI), denominate: SARI Enterprise e SARI Real-Time, in uso alla Direzione Centrale Anticrimine CUP F89D19000100006 - CIG 85092230F6. Available here

Avviso per manifestazione d'interesse relativa all'acquisizione di apparecchiature hardware e software finalizzate a potenziare le attuali funzionalità e prestazioni delle due componenti del Sistema Automatico Riconoscimento Immagini (SARI), denominate: SARI Enterprise e SARI Real-Time, per le esigenze della Direzione Centrale Anticrimine della Polizia di Stato. Available here

European Digital Rights (EDRi), Respecting fundamental rights in the cross-border investigation of serious crimes A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II"), 7 September 2022. Available here

Filippo Sensi, interrogazione a risposta immediata "Intendimenti in ordine all'utilizzo di sistemi di riconoscimento facciale, anche in relazione alla necessaria tutela dei diritti fondamentali della persona – n. 3-02074

Polizia di Stato, Brescia: ladri d'appartamento scoperti grazie al riconoscimento facciale, 07 September 2018

Comando Generale dell'Arma dei Carabinieri, Approvvigionamento n.4 sistemi "Face Recognition" per le esigenze operative dei Reparti dell'Arma dei Carabinieri-Avviso aggiudicazione appalto.

Comando Generale dell'Arma dei Carabinieri - Pagamenti 1° Trimestre 2022.

Guardia di Finanza, Acquisto di un prodotto software per il foto-segnalamento e servizi correlati.

Vrije Universiteit, Call for PhD researcher on Criminal Procedure Law and AI for intelligence analysis. Available here

Rijksoverheid, *Letter of the Minister of Justice and Security of the Netherlands to MPs to Inform Them About the Use of Facial Recognition Technology by Law Enforcement Agencies (in Dutch)*, 20 November 2019

U.S. Department of Commerce National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (December 2019) and Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification (August 2017)*