Computer Law & Security Review 56 (2025) 106092

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Facial recognition technology in law enforcement: Regulating data analysis of another kind

Monika Simmler, Giulia Canova *

Competence Center for Criminal Law and Criminology, University of St. Gallen, Bodanstrasse 3, 9000 St Gallen, Switzerland

ARTICLE INFO

Keywords:
Facial recognition
Law enforcement
Biometric identification systems
Digital investigations
Data analysis

ABSTRACT

Facial recognition technology (FRT) has emerged as a powerful tool for law enforcement, enabling the automated identification of individuals based on their unique facial features. Authorities have more and more made use of the technology to enhance criminal investigations through the analysis of images and video footage. In view of its increased use in Europe, this paper explores the legal implications of FRT in law enforcement under EU law and evaluates approaches to regulation. FRT use constitutes biometric data processing and comes with a particularly sensitive analysis of data. Its specific nature is grounded in the creation of a new (biometric) quality of data in order to subsequently compare for matches. Due to its impact on fundamental rights, this approach differs from conventional forensic analyses and must be appropriately regulated. Such regulation should consider the multiple data processing steps and reflect each step's impact on fundamental rights. From this procedural stance, the shortcomings of the EU Artificial Intelligence Act (AI Act) become evident. The AI Act contains specific rules for biometric AI systems but does not provide the necessary legal bases to justify FRT use by law enforcement. Without a comprehensive legal framework, such use is not permitted. This article provides concrete guidelines for addressing such regulation.

1. Introduction

Facial recognition technology (FRT) might be one of the most powerful applications of Artificial Intelligence (AI) for law enforcement and surveillance practices.[1] It enables the automated comparison of human faces and can be used in law enforcement to identify individuals related to criminal activities (e.g., persons suspected of having committed a crime). By 2021, at least 11 out of 27 Member States of the EU leveraged the potential of FRT in the context of criminal investigations.[2]

The increasing use of FRT by public authorities, especially in law enforcement, has not been without controversy, above all due to its relation to fundamental rights and risks regarding (illegitimate) surveillance.[3] In a first judgement concerning FRT use by law enforcement, the European Court of Human Rights (ECtHR) held that authorities' use of FRT to analyse CCTV footage and social media images to identify a protester violated fundamental rights.[4]

Due to its risks for fundamental rights, FRT has moved into the regulatory spotlight.[5] In August 2024, the EU Artificial Intelligence Act (AI Act) entered into force, introducing a new regulatory regime for AI

* Corresponding author.
E-mail addresses: monika.simmler@unisg.ch (M. Simmler), giulia.canova@unisg.ch (G. Canova).

[1] Giuseppe Mobilio, 'Your face is not new to me – Regulating the surveillance power of facial recognition technologies' (2023) 12(1) Internet Policy Review <https://doi.org/10.14763/2023.1.1699> accessed 30 September 2024; Kevin W. Bowyer, 'Face recognition technology: security versus privacy' (2002) 23(1) IEEE Technology and society magazine 9.

[2] Francesco Ragazzi et al., 'Biometric and behavioural mass surveillance in EU member states: report for the Greens/EFA in the European Parliament' (2021), 38 <https://hdl.handle.net/1887/3256585> accessed 30 September 2024.

[3] See e.g., European Agency for Fundamental Rights (FRA) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2020) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 19 July 2023; Desara Dushi, 'The use of facial recognition technology in EU law enforcement: Fundamental rights implications' (2020) <https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content> accessed 30 September 2024.

[4] Glukhin v. Russia, App No. 11519/20 (ECtHR, 3 July 2023).

[5] Irena Nesterova, 'Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world' (2020) 74 SHS Web of Conferences 1.

https://doi.org/10.1016/j.clsr.2024.106092

Available online 29 November 2024

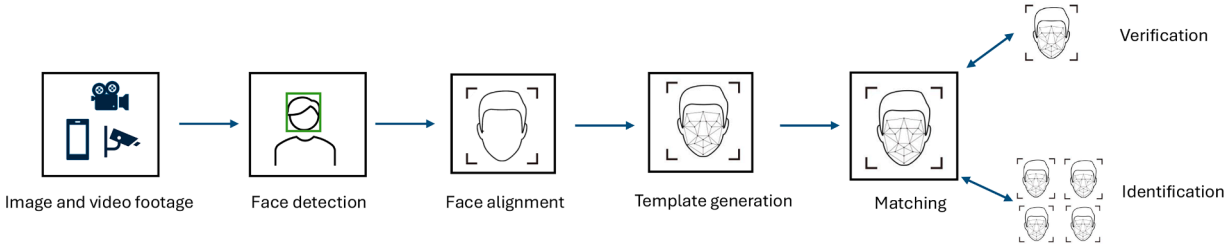

Fig. 1. Basic facial recognition process.

systems, including biometric identification systems.[6] However, as yet there has been little research examining the regulation from a law enforcement perspective or evaluating how these rules might govern FRT use in criminal proceedings (i.e., for the investigation of crimes).[7]

Against this backdrop, this paper explores the legal implications of FRT use by law enforcement and elaborates key aspects of FRT regulation in light of the AI Act. The use of FRT involves particularly sensitive data analyses creating data of a new nature, therefore representing data analyses of another kind. The goal is to provide guidance on how to regulate FRT based on this understanding. To this end, we first outline the technical functionality of FRT and differentiate among various uses by law enforcement (Ch. 2). Following that, we illustrate why FRT use must be understood as multi-step data processing, accompanied by multiple serious interferences with fundamental rights (Ch. 3). We then introduce relevant aspects of regulation and appraise the rules of the AI Act, considering the previously established framework (Ch. 4). To conclude, we summarise the key aspects of a regulatory framework for FRT in law enforcement. The approach developed can serve as a regulatory framework for FRT, but also the deployment of other forms of advanced technology.

2. Facial recognition technology: A powerful tool for law enforcement

2.1. Technical foundations

In general, facial recognition refers to the process of identifying or confirming an individual's identity based on their facial features. Naturally done by humans, this task can also be performed by machines, namely through FRT.[8] The technology is a classic biometric one, based on the identification of an individual's biological or behavioural features, like fingerprint, iris, voice or signature.[9] Just as with any other biometric technology, facial recognition systems operate in two different ways: identification and verification.[10] Facial identification operates on the basis of a one-to-many match (1:n). In this procedure, a captured face is compared with multiple faces in a database. In contrast, facial verification is based on a one-to-one match (1:1), where one face is matched against another single face to validate the identity that is claimed.[11] For both purposes, the facial recognition procedure deals with a visual pattern recognition problem, where a three-dimensional object – the human face – must be identified.[12] The facial recognition approach has been significantly transformed by the development of AI and deep learning,[13] which makes FRT an application of "smart criminal justice".[14]

In its early development stage from the 1960s on, FRT operated with algorithms to analyse the geometric structure of the face.[15] Traditional facial recognition methods relied on comparing specific features of the face (e.g., by measuring the geometrical location of facial points like nose, eyes or mouth) and were later on combined with machine learning techniques (such as principal component analysis or support vector machines) to process facial features. Recently, traditional FRT has been superseded by deep learning methods based on neural networks which are trained with large datasets and able to learn the relevant facial features from the data.[16] Modern facial recognition systems thus involve AI techniques that are applied to solve the recognition problem.[17] This contribution explores the use of such modern FRT based on AI.

Facial recognition systems follow a basic process that consists of several steps (see Fig. 1). First, the system is supplied with images or videos of faces.[18] Second, the system detects the existence of human faces in the material provided by examining whether and where distinct objects (in this case, human faces) are visible in the data.[19] Third, the detected faces are aligned by a set of reference points at fixed locations in the image.[20] Fourth, the identified features of a face are extracted and transformed into a digital template.[21] Fifth, the extracted template is

[6] Irena Barkane, 'Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance' (2022) 27(2) Information Polity 147, 152 et seq.; Sara Solarova et al., 'Reconsidering the regulation of facial recognition in public spaces' (2022) 3 AI and Ethics 625.

[7] See only Vera Lucia Raposo, 'The use of facial recognition technology by law enforcement in Europe: a non-orwellian draft proposal' (2022) 29 European Journal on Criminal Policy and Research 515.

[8] Alice J. O'Toole and Carlos D. Castillo, 'Face Recognition by Humans and Machines: Three Fundamental Advances from Deep Learning' (2021) 7 Annual Review of Vision Science 543, 544.

[9] Lixian Li, Xiaohui Mu, Siying Li and Haipeng Peng, 'A review of face recognition technology' (2020) 8 IEEE access 139110; Anil K. Jain and Arun Ross, 'Handbook of Biometrics' (Springer 2008), 4; Catherine Jasserand, 'Legal nature of biometric data: From generic personal data to sensitive data' (2016) 2 (3) European Data Protection Law Review 297, 309.

[10] Stan Z. Li and Anil K. Jain, 'Handbook of face recognition' (Springer 2011), 2.

[11] Li and Jain (n 10) 2 et seq.; Davide Castelvecchi, 'Is facial recognition too biased to be let loose?' (2020) 587 Nature 347, 348.

[12] Li and Jain (n 10) 3.

[13] Li, Mu, Li and Peng (n 9) 139113.

[14] Monika Simmler, Simone Brunner, Giulia Canova and Kuno Schedler, 'Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system' (2023) 31 Artificial Intelligence and Law 215.

[15] Li, Mu, Li and Peng (n 9) 139111.

[16] Daniel Saez Trigueros, Li Meng and Margaret Hartnett, 'Face Recognition: From Traditional to Deep Learning Methods' (2018) <https://arxiv.org/abs/1811.00116> accessed 30 September 2024; Waqar Ali et al. 'Classical and modern face recognition approaches: a complete review' (2021) 80 Multimedia Tools and Applications 4825, 4838 et seq.

[17] Li, Mu, Li and Peng (n 9) 139111 et seq.

[18] Isabelle Hupont, Songül Tolan, Hatice Gunes and Emilia Gómez, 'The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems' (2022) Scientific Reports <https://doi.org/10.1038/s41598-022-14981-6> accessed 30 September 2024.

[19] Li and Jain (n 10) 4; Ahmad Tolba, Ali El-Baz and Ahmed A. El-Harby, 'Face recognition: A literature review' (2005) 2(2) International Journal of Signal Processing 88; Mejda Chihaoui, Akram Elkefi, Wajdi Bellil and Chokri Ben Amar, 'A Survey of 2D Face Recognition Techniques' (2016) 5(4) Computers 2.

[20] Saez Trigueros, Meng and Hartnett (n 16).

[21] Saez Trigueros, Meng and Hartnett (n 16); Chihaoui, Elkefi, Bellil and Ben Amar (n 19).

matched against one or many biometric templates of registered faces.[22] This matching enables the actual "recognition" of a face,[23] for which the similarity of the faces is calculated mathematically. If the matching process establishes a mathematical similarity in the range of a certain tolerance threshold, the faces are recognized as identical and the system reports a match.[24] Thus, FRT produces a similarity comparison of a distinct face to that of other faces.[25]

Due to its probabilistic nature, FRT does not deliver definite results, but rather probability measures about the similarity of faces.[26] The quality of FRT is inevitably linked with the accuracy of the technology being used. Since with state-of-the-art FRT 100 % accuracy cannot be guaranteed, its use can result in false positives (when a face is wrongly matched with another face) and false negatives (when a face is wrongly not recognized as match).[27] The most popular facial recognition algorithms are estimated to achieve accuracy rates of around 90 %.[28]

2.2. Application in practice

2.2.1. Type of matching

FRT supports the identification of individuals and can therefore be of great use to law enforcement authorities (i.e., the police, public prosecution, and ultimately, the courts). FRT allows for the automated identification of individuals that may in some way be related to criminal events, such as suspects, wanted persons, victims or witnesses.[29] The most valuable type is face identification (1:n matching), which allows for the identification of individuals by comparing facial images with those in databases.[30]

There are different types of databases used for the matching. Most commonly input data are matched against government-stored data (e.g., national biometric databases of previously identified individuals like mugshot databases or specific watchlists of wanted persons). The type of government-stored data may be restricted to police databases but can also include other databases including driver license or passport photos.[31] Additionally, it is possible to use databases consisting of surveillance footage or private data sources, such as footage from electronic devices. Lastly, open-source data can be used, particularly images made public on the internet and social media. For instance, the facial recognition software "Clearview AI" operates a database of about three billion images that have been published online.[32]

2.2.2. Prevention or repression

FRT in law enforcement can be used for both preventive and repressive purposes; each accompanied by different legal implications. For prevention, FRT is used for general surveillance of publicly accessible spaces.[33] To this end, existing video surveillance infrastructure is equipped with FRT to automatically analyse persons passing through monitored areas, often in real-time.[34] Such surveillance is neither linked to the suspicion of a concrete crime nor connected to an imminent threat of a concrete danger or disruptive incident. From 2017 to 2018, German authorities tested FRT for such purposes at the Berlin Südkreuz train station, scanning the faces of individuals entering a specific area.[35] Furthermore, FRT can be used for specific preventive surveillance purposes, where it is linked to the existence of a concrete threat to public safety. Monitoring protests to observe and immediately identify rioters is an example of a use falling within this category.[36]

Repressive purposes refer to actions taken to prosecute criminal offences (i.e., in the aftermath of a crime). In this context, FRT is used for the identification of persons related to a criminal event.[37] It is used on an ex-post basis to analyse data. However, in criminal investigations, FRT can also be used in real-time, namely for the location and detainment of wanted or suspected persons. Real-time systems extract biometric data from "live" material and instantaneously match them against a database.[38] For this purpose, surveillance infrastructure can be designed to match the faces of individuals passing through a specific area (e.g., a stadium).[39] Such applications of FRT for investigative purposes (ex-post and real-time) are slowly but consistently spreading in Europe.[40] The present work focuses on this area and examines the fundamental rights implications of FRT use in criminal proceedings.

3. Facial recognition technology as multi-step data processing

3.1. A procedural perspective on technology use

As seen, the facial recognition process consists of several steps. To address the legal implications, a procedural understanding of FRT application is necessary. The use of FRT represents a chain of events with multiple components. Since every process step may be relevant, it is necessary to deconstruct the sequence into its individual parts and assess the implications per step. Only in this way can the legal relevance of FRT use be properly determined.

As indicated, this article focuses on FRT use for repressive purposes, involving cases where a criminal investigation has been formally opened according to the relevant criminal procedural rules. The use of FRT in criminal investigations is an application of digital investigations, (i.e., one involving information and communication technologies). In general, digital investigations are based on the following steps: (1.) collection, (2.) analysis, and (3.) exploitation of data. In practice, these process steps are often run in multiple cycles. They can be conceptualized as multi-step processes, wherein data are collected, analysed, and exploited to contribute valuable information to a criminal investigation. Digital investigations can be structured as process sequence similar to a value chain (see Fig. 2). A value chain is a set of activities carried out to achieve value. Originally introduced to illustrate how companies create value, the procedural concept can also be adapted for other processes that generate output across several steps.[41]

A value chain perspective helps to illustrate the data processing steps

[22] Li and Jain (n 10) 4.
[23] Chihaoui, Elkefi, Bellil and Ben Amar (n 19).
[24] Li and Jain (n 10) 4; Hupont, Tolan, Gunes and Gómez (n 18).
[25] Bowyer (n 1) 11.
[26] FRA (n 3).
[27] Tambiama Madiega and Hendrik Mildebrath, 'Regulating facial recognition in the EU' (2021) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf> accessed 30 September 2024; Joy Buolamwini and Timnit Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81(1) Proceedings of Machine learning Research 1.
[28] Buolamwini and Gebru (n 27) 9.
[29] Kristine Hamann and Rachel Smith, 'Facial Recognition Technology' (2019) Criminal Justice 9, 9.
[30] Cf. Castelvecchi (n 11) 348.
[31] Ragazzi et al. (n 2) 38.
[32] Isadora Neroni Rezende, 'Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective' (2020) 11(3) New Journal of European Criminal Law 375, 376.
[33] Hamman and Smith (n 29) 10.
[34] Mario Martini, 'Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit' (2022) 41(1-2) Neue Zeitschrift für Verwaltungsrecht – Extra 4, 1.
[35] Martini (n 34) 8.
[36] Privacy International 'How facial recognition technology can be used at a protest' (2021) <https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest> accessed 30 September 2024.
[37] Madiega and Mildebrath (n 27) 3.
[38] ibid 3.
[39] Behrooz Kamgar-Parsi, Wallace Lawson and Behzad Kamgar-Parsi, 'Toward development of a face recognition system for watchlist surveillance' (2011) 33 (10) IEEE Transactions on Pattern Analysis and Machine Intelligence 1925.
[40] Ragazzi et al. (n 2) 38.
[41] Cf. Michael E. Porter, 'The Competitive Advantage: Creating and Sustaining Superior Performance' (Free Press 1985), 36 et seq.

Fig. 2. Process steps of digital investigations.

necessary to generate valuable information in criminal investigations.[42] The process produces certain criminalistic value. Deploying technologies supports this value creation in a unique way. Capturing the nature and legal relevance of technology use in law enforcement is facilitated by understanding it not just as tool but as the procedure it implies. This is crucial because the process not only reflects value creation but is equally accompanied by various possible encroachments on the fundamental rights of affected individuals.

FRT use in law enforcement can be structured according to the process steps of digital investigations. First, data in the form of facial images is collected. Second, the data is analysed by a biometric-technical procedure in which facial features are extracted and transformed into biometric templates and subsequently matched against a database. This is the step of the data analysis in which the technology is deployed and "facial recognition" in a narrower sense takes place. Third, the generated information is exploited to find use in the investigation (e.g., by triggering further investigative measures based on the identification or disclosure of the data to other authorities). Of course, each step can be further subdivided. Key, however, is to capture the procedural nature of such technology deployment in order to elaborate upon the legal implications of the data processing steps.

3.2. *Fundamental rights implications*

FRT in criminal proceedings contributes to investigations through the identification of individuals. Data is collected, analysed, and the information generated further exploited. From a legal perspective, the use of FRT amounts to governmental data processing.[43] Thus, it appears equally as value and "exposure chain," during which individuals are exposed to multiple data processing steps by authorities (and therefore, interferences). The impact of each processing step on fundamental rights must be assessed.

The legal assessment is concerned with the right to respect for private life and the right to protection of personal data, two fundamental pillars of the European fundamental rights framework.[44] Similarly, European states guarantee in their constitutions for the right to personal privacy[45] or the right to information privacy.[46] In EU law, the protection of fundamental rights is based on the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (CFREU). Article 8 ECHR guarantees the "right to respect for private and family life", encompassing the protection from unwanted collection, access and use of personal data.[47] Similar, Article 7 CFREU guarantees the "right to respect for his or her private and family life". Under Article 8 CFREU, the fundamental right to "protection of personal data concerning him or her" has been introduced as stand-alone, innovative fundamental right.[48] Article 16 of the Treaty on the Functioning of the European Union (TFEU) nearly identically guarantees the right to protection of personal data and mandates the European Parliament and the Council to lay down rules relating the protection of individuals with regard to the processing of personal data by EU institutions and Member States when they are acting under the scope of EU law.

For the legal assessment, it is relevant that FRT operates with facial images of natural persons.[49] Facial images depict physical factors of natural persons and thus constitute personal data, i.e. information relating to identified or identifiable individuals. FRT comes with the processing of personal data and thus falls under the scope of Article 8 ECHR[50] and Article 7 and Article 8 (1) CFREU.

Data protection is further specified by secondary EU legislation, namely the Regulation 2016/679 ("General Data Protection Regulation", GDPR) and the Directive 2016/680 ("Law Enforcement Directive", LED), the latter of which being the specific legal framework for data protection in law enforcement. The LED applies to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, and prosecution of criminal offences and the execution of criminal penalties (Article 1 (1) LED). Data protection in law enforcement is specifically regulated under EU law, even though the Union's competence in the field of law enforcement is limited to measures concerning the cooperation of police authorities, the mutual recognition of decisions and – if necessary – the harmonisation of criminal law.[51] However, as is the case with the LED, law enforcement can be regulated based on other competences, such as the data protection competence of the EU (Article 16 (2) TFEU).[52] Due to the LED's nature as an EU Directive, the rules require transformation into national law.[53] Still, they are binding and set overarching requirements for data processing, also for FRT in law enforcement.

[42] See for another attempt to conceptualize a data value chain, Abou Zakaria Faroukhi, Imane El Aloui and Youssef Gahi, 'Big data monetization throughout Big Data Value Chain: a comprehensive review' (2020) 7 Journal of Big Data <https://doi.org/10.1186/s40537-019-0281-5> accessed 30 September 2024.

[43] FRA (n 3) 23 et seq.; European Data Protection Board (EDPB), 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0' 14 <https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf> accessed 30 September 2024.

[44] Herke Kranenborg, 'Article 8 – Protection of Personal Data' in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (Eds.), The EU Charter of Fundamental Rights – A Commentary (2nd Edition Nomos 2022); Gloria González Fuster and Raphaël Gellert, 'The fundamental right of data protection in the European Union: in search of an uncharted right' (2012) 26(1) International Review of Law, Computers & Technology 73.

[45] See Article 18 of the Spanish Constitution of 1978.

[46] See Article 2 (1) in conjunction with Article 1 (1) of the Basic Law for the Federal Rebublic of Germany of 1949.

[47] Pamela McCormick, Clare Ovey and Bernadette Rainey, 'The European Convention on Human Rights' (8th Edition Oxford University Press 2021), 377.

[48] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data' (2017) Big Data & Society 4, 1; Mads Anednas and Stefan Zleptnig, 'Surveillance and Data Protection: Regulatory Approaches in the EU and Member States' (2003) 14 (6) European Business Law Review 780.

[49] Hupont, Tolan, Gunes and Gómez (n 18); EDPB (n 43) 10 et seq.

[50] Glukhin v. Russia (n 4) para 73.

[51] Helmut Satzger, 'International and European Criminal Law' (2nd Edition Beck 2018), 125; Werner Schroeder, 'Limits to European Harmonisation of Criminal Law' (2020) 2 EuCrim 144, 145; Matthias Valta and Johann Justus Vasel, 'Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz' (2021) 5 Zeitschrift für Rechtspolitik 142, 143.

[52] For this development see Kristin Pfeffer, 'Stille Europäisierung – Wie europäisch wird das deutsche Polizeirecht' (2022) 5 Neue Zeitschrift für Verwaltungsrecht 294.

[53] M.R. Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5(3) European Data Protection Law Review 367, 368.

3.2.1. Data collection

The initial collection of facial images (e.g., through the seizure of data from electronic devices and CCTV footage) represents collection of personal data (Article 3 (1) and (2) LED) and constitutes an interference with Article 8 ECHR as well as Article 7 and Article 8 CFREU.[54] This applies to the collection of facial images of individuals being identified, but also for the collection of the n images in databases used.

Article 8 (1) of the LED sets the general rule for data processing, stating that Member States shall provide for processing only to the extent that such processing is necessary for the performance of a task carried out by a competent authority for purposes set out in Article 1(1) LED, and that it is based on Union or Member State law. This means that processing must be necessary for the prevention, investigation, or prosecution of offences or the execution of sanctions (Article 1(1) LED) and provided for by the law.[55] Following that, the collection of facial images for the FRT process constitutes an interference and thus requires a legal basis in Union or Member State law. The legal basis does not necessarily have to be a legislative act adopted by a parliament, but it must be clear and precise and its application foreseeable to persons subject to it (recital 33 LED). Regarding the content of the legal basis, Article 8 (2) LED requires the concrete objective and purpose to at least be specified, as well as the type of personal data being processed (Article 8 LED).

The intensity of the interference accompanying the collection of data for FRT can vary. The specific objective and type of personal data must be considered (as referenced in Article 8 (2) LED). Additionally, the data subjects affected (e.g., persons who are suspected of a crime or persons who have not given cause to be subject to any measure) and the awareness of the affected individuals are both relevant. For instance, data collection affecting a large number of non-suspected persons without any notification is particularly invasive.[56] In sum, data collection for the FRT process not only requires a legal basis, but specific legal bases that precisely regulate the circumstances of the data collection and the specific purpose for which it is collected.[57]

3.2.2. Data analysis

Data collection is followed by data analysis. This is the step in the process where in a narrower sense the technology (i.e., the facial recognition software) comes into use. The analysis itself consists of two sub-steps: biometrical measurement of facial images and their matching against a database. The first sub-step, the extraction of biometric features, produces biometric templates, and with that generates biometric data from personal data.

Therefore, within this step, processing delves into the area of biometric data, a particularly sensitive type that is granted special protection.[58] The LED assigns biometric data to a special category of personal data (Article 10 LED) and its processing amounts to a severe interference.[59] Such particularly sensitive data merit specific protection (i.e., requirements of strict necessity and additional safeguards), as the context of their processing is liable to create significant risks to fundamental rights.[60]

Article 3 (13) LED defines biometric data 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." Not every use of facial images constitutes specific technical processing of this kind.[61] The decisive element is the technical analysis of biometric facial features and generation of the biometric templates being matched against databases.

FRT analysis generates biometric data from mere personal data (e.g., facial images), and with that generates templates of a new quality of data that allow for the identification of individuals. Due to the sensitive nature of the new data generated, this step constitutes another serious interference.[62] This is what makes FRT unique and distinguishes it from common data analysis techniques such as searching electronic devices and bare data mining. FRT does not just analyse data, it first creates new data that is then matched against a database in order to create investigative value.

Article 10 LED sets a special protection regime for the processing of biometric data used for identification purposes. It is important to note that Article 10 LED only mentions processing for the purpose of uniquely identifying a natural person. Such identification involves one-to-many (1:n) matching and requires a database. Hence, the processing of biometric data for verification purposes (to verify and confirm whether an individual is the same person as he/she claims to be), where one single template is matched against another template (1:1 matching), would not fall under such protection.[63]

Notwithstanding, for identification purposes, Article 10 LED states that processing is only allowed when (cumulatively): (i) strictly necessary, (ii) subject to appropriate safeguards for the rights and freedoms of the data subject, and only (iii) (alternatively) (a) where authorised by Union or Member State law, (b) to protect the vital interests of the data subject or another natural person, or (c) where such processing relates to data that are manifestly made public by the data subject. This regime reflects the sensitivity of biometric procedures and is justified by the potentially drastic consequences that misuse would have for individuals.[64] Certain issues raised in relation to FRT vividly show this. In the case of FRT, the risk of misuse is strongly linked with the accuracy of the system in use, which can have high rates of false positives or false negatives and be subject to bias.[65] Biases within the system can lead to discriminatory effects against certain groups of people; for instance, studies have identified reduced accuracy for people of colour and women.[66] Inaccurate results from these biometric procedures can have drastic consequences, especially if leading to wrongful accusation.

The severity of FRT procedures is also due to the dispersion of the analysis. It not only affects individuals targeted for identification, but also all n persons whose biometric data is stored in the matching database and biometrically processed, too. The interference does not depend on the outcome of the matching process (e.g., a positive match).[67] The biometric analysis also constitutes a serious interference if the matching results in a "no-hit," and even if the biometric template is immediately deleted after the analysis.[68] The dispersion of the interferences accompanying the biometric analysis and matching (particularlysuch in real-time based on video surveillance) also justifies concerns about large-scale surveillance.[69]

[54] Hannover v. Germany, App No. 59320/00 (ECtHR, 24 June 2004) paras 76–78; EDPB (n 43) 13 et seq.

[55] Leiser and Custers (n 53) 371 et seq.

[56] On the relevance of the covertness of measures Christian Rückert, 'Zwischen Online-Streife und Online-(Raster-)Fahndung' (2017) 129(2) Zeitschrift für die gesamte Strafrechtswissenschaft 320.

[57] EDPB (n 43) 44.

[58] Jasserand (n 9) 297; Raposo (n 7) 2.

[59] Court of Justice of the European Union (CJEU), Case c-205/21, Judgment of the Court (Fifth Chamber) of 26 January 2023, Criminal proceedings against V.S., Request for a preliminary ruling from the Spetsializiran nakazatelen sad (ECLI:EU:C:2023:49), para 116.

[60] ibid, para 116.

[61] See E.J. Kindt, 'Having yes, using no? About the new legal regime for biometric data' (2018) 34 Computer Law & Security Review 523, 526.

[62] EDPB (n 43) 14.

[63] See Kindt (n 61) 526 et seq.

[64] Jasserand (n 9) 307.

[65] Madiega and Mildebrath (n 27) 7.

[66] Buolamwini and Gebru (n 27) 9.

[67] See EDPB (n 43) 14.

[68] EDPB (n 43) 14, see also Federal Constitutional Court of Germany BVerfG 150, 244, "Kfz-Kennzeichen".

[69] Solarova (n 6) 172; Barkane (n 6) 153.

Data analysis performed with FRT is of a special nature and has a severe impact on fundamental rights. It is, thus, demanding specific legal protection. Of legal relevance is the biometric measuring of faces, as well as the recognition itself. The sensitive nature of the data being created and subsequently matched makes for the very special character of the data analysis.

3.2.3. Data exploitation

Following the data analysis, the data is exploited by the authorities for the investigation of crimes, e.g., by identifying suspected individuals from footage or confirming the presence of a person at a crime scene. It should be acknowledged that any further use of personal data interferes with Article 8 ECHR once more.[70] This applies not only to the concrete use of the data as evidence, but also to its mere storage or retention in databases, and even more so for disclosure of the data.[71] Particularly the retention of previously analysed biometric data (like fingerprints, facial images or iris scans) of citizens is delicate as it enables the identification of individuals for future investigations.[72] The retention must be proportionate to the initial purpose for which the data has been collected and must be limited in time.[73] Systematic retention of biometric data entered in governmental databases means severe interferences for a large number of people and is only allowed if strictly necessary.[74]

In addition to retention of collected data, it is relevant if and to what degree the exploitation of the data comes with disclosure of this data to other authorities and/or third parties.[75] Disclosure of data (i.e., by transmission, dissemination or otherwise making available) to public authorities or other bodies constitutes additional processing of the data.[76] Exploitation of such data must be acknowledged as an additional data processing step, and from a fundamental rights perspective, as additional (potentially severe) interference. This applies to the exploitation of the biometric templates generated, but also to the results produced by the biometric analysis itself.

3.3. Summary

FRT use in law enforcement entails multi-step data processing, and each of the steps must be viewed as an interference with Article 8 ECHR (as well as Article 7 and Article 8 (1) CFREU). The first step involves the collection of personal data in the form of facial images, which must be lawful and requires a legal basis (Article 8 (1) LED). The second step, the data analysis, entails a biometric analysis of the collected facial images and subsequent matching of the generated biometric data with databases. The biometric analysis as well as the matching of the data constitute severe interferences with Article 8 ECHR (as well as Article 7 and Article 8 (1) CFREU). The data analysis constitutes biometric data processing and falls under the enhanced protection regime of Article 10 LED. As such, the use of FRT is only allowed if strictly necessary, specifically provided for in legal bases and accompanied by appropriate safeguards. Additionally, any subsequent exploitation of the data such as its use as evidence in proceedings, retention in a database or disclosure to other authorities amounts to an additional processing step and consequently an interference with Article 8 ECHR (as well as Article 7 and Article 8 (1) CFREU) that must likewise be grounded in a legal basis.

4. Approaching regulation: AI Act and beyond

4.1. Key aspects of regulation

Making use of FRT in law enforcement impacts fundamental rights in multiple ways and requires an appropriate legal framework. The framework chosen must reflect the entirety of data processing, from the input data consisting of facial images to the actual use of the insights gained by biometric analysis. The law must be sufficiently clear to give citizens an adequate indication of the circumstances in which authorities are empowered to resort to interferences.[77] This applies to each of the steps that are equally of investigative value from the authorities' perspective and exposure of the individuals affected.

Criminal procedure codes provide a variety of legal norms for data collection. Examples include the generation of identification data (like mugshots, DNA profiles or fingerprints)[78] and the seizure of electronic devices (that for instance contain stored images).[79] However, the invocation of legal bases for the collection of facial images does not suffice to justify the biometric data processing FRT implies. Every step interfering with fundamental rights must be provided for by the law.[80] In other words, every step of the FRT process must be considered in regulation. Next, we therefore present the relevant aspects that should be considered in a legal framework for FRT use in criminal investigations along the "value chain."

4.1.1. Data collection

A legal framework for FRT in law enforcement must entail legal bases for the collection of data (i.e., the pictures and footage to be analysed). More precisely (and valid actually for any regulation of data processing), it is necessary to regulate: (1) the *type of data* that is collected, (2) *sources* of the data collected, (3) categories of *individuals affected* by the collection, (4) *recognizability* or covertness of the collection, and (5) for what specific *purpose* the data are ultimately collected.

First, a legal framework must specify the *type of data* collected (i.e., whether non-personal, personal, or particularly sensitive data is collected). In case of FRT, facial images are collected, which in their original form represent personal data.[81]

Second, it is important to regulate the *source* of the input data. For FRT, a regulation must differentiate whether facial images are gathered from lawfully established criminal or governmental databases (e.g., police records containing images from previously suspected or convicted individuals), CCTV footage of public spaces, seized electronic devices, or publicly accessible sources on the internet and social media.[82] This applies to both the images of persons to be identified and databases used for matching.

Third, the categories of *individuals affected* must be considered.[83] Here, it is important to determine whether data is collected from persons because there are grounds for being targeted (e.g., because they are suspected of having committed a criminal offence or because they are alleged victims), whether the measure is aimed at specific persons

[70] S. and Marper v. United Kingdom, App No. 30562/04 and 30566/04 (ECtHR 4 December 2008) para 84 and 86.
[71] See also Article 3(2) LED.
[72] S. and Marper v. UK, para 119 et seq.; see also Kindt (n 61) 527 and 530.
[73] S. and Marper v. UK, para 119 et seq.; see also Kindt (n 61) 527.
[74] CJEU c-205/21 (n 59) paras 133–135.
[75] European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights' (2022) N 223 ff. <https://www.echr.coe.int/documents/d/echr/guide_art_8_eng> accessed 30 September 2024.
[76] See Article 3(2) LED; on the conditions for access and further use of data under the LED see also Catherine Jasserand 'Subsequent Use of GDPR Data for a Law Enforcement Purpose' (2018) 4 European Data Protection Law Review 152, 162.
[77] Sunday Times v. the United Kingdom, App no. 6538/74, (ECtHR 26 April 1979), para 49.
[78] See e.g., §§ 81b et seq. of the German Criminal Procedural Code; Article R40-26 of the French Criminal Procedural Code.
[79] See e.g., §§ 94 et seq. of the German Criminal Procedural Code; Article 97 et seq. of the French Criminal Procedural Code.
[80] Jens Meyer-Ladewig, Martin Nettesheim and Stefan von Raumer, 'EMRK, Europäische Menschenrechtskonvention' (5th Edition Nomos 2023), Article 8 N 102.
[81] Cf. EDPB (n 43) 34 et seq.; see also Article 6 (a) LED.
[82] Raposo (n 7) 8 et seq.
[83] CJEU c-205/201 (n 59) paras 82 et seq.

disturbing public safety or order, or whether the measure affects individuals without cause. If a high number of non-suspect individuals is affected, there is a graver impact on fundamental rights, and this must be considered by regulation.[84]

Fourth, the *recognizability* of the data collection is relevant (i.e., the data subject's knowledge of the measure).[85] Information about the data processing is a prerequisite if data subjects are to exercise their data protection rights.[86] In an FRT context, data collection (and analysis) is usually carried out without the knowledge of the data subject, increasing the intensity of the interference. Due to the severity of the interferences accompanying covert measures, criminal procedural codes usually provide specific rules for covert investigations.[87] FRT regulation should thus reflect this aspect of recognizability by providing specific rules about notification and effective legal remedies as compensation.

Lastly, facial images are to be collected for a *specific purpose* defined by law.[88] Considering FRT in criminal proceedings, there must be legal bases that authorize the collection of facial images to be used in criminal investigations.

4.1.2. Data analysis

The chain's second element, data analysis, requires special regulatory consideration. The analysis performed by facial recognition software is particularly invasive. Solely setting standards for data collection without further specifying the regulation of subsequent analyses does not suffice. Some Member States provide legal bases for single aspects of FRT use in law enforcement, e.g., the automatic comparison of images with national identification databases.[89] This is not enough to regulate the sensitive data analyses. Serious interferences must be foreseen in legislation with a high degree of certainty and clarity. Vague norms generally allowing for the comparison of identification data are not sufficient. Moreover, the European Data Protection Board (EDPB) has adopted guidelines on the use of FRT in the area of law enforcement to promote common understanding of the EU data protection laws that serve as soft law in that regard. These guidelines, for instance, lay out the relevant rules of the LED regarding FRT use in law enforcement.[90] However, they are intended as guidelines and not legally-binding for Member States. Comprehensive legal frameworks covering the data analysis performed by FRT have not yet been developed.

Regarding the data analyses performed by FRT, several aspects are legally relevant, including: (1) the *method* of analysis, (2) *technological capacities* of the software used, (3) *datasets* involved, and (4) *timing* of the analysis.

First, the *method* of analysis itself has regulatory consequences. There are forensic analyses that simply search data for specific content. Such 'light' forms of data analysis are not particularly invasive, as they do not change the quality of the data. Slightly more invasive are analyses that structure or reorganize data or combine it with other datasets, as this amounts to additional data processing. Particularly intrusive are data analyses that change the quality of the data, especially if sensitive data is newly generated. With FRT, generic personal data is transformed into biometric data,[91] adding informative value but also making the data particularly sensitive. This must be reflected in legal provisions that indicate that new biometric data (in the form of facial templates) are generated for matching in a subsequent step. Therefore, the processing of biometric data for identification demands appropriate safeguards to prevent their misuse.[92] Safeguards usually contain technical, organisational, and procedural requirements.[93] Technical requirements call for qualitative standards regarding the data and technology in use.[94] Organisational safeguards often include oversight by an independent authority.[95] Procedural safeguards should ensure that persons whose biometric data has been analysed have effective legal remedies to challenge the results.[96]

As a second factor, the *capacities* of the technology in use have implications for regulation. FRT operates based on AI, which can be subject to bias and discriminatory effects, and 100 % accuracy can never be guaranteed.[97] AI systems and their accuracy depend on the datasets used to train the tools.[98] Low-quality data such as incomplete or biased information can lead to low-quality outcomes, which in turn risk violation of fundamental rights.[99] The risk of bias and quality of datasets must therefore be addressed in a regulatory framework.

Third, matching with *datasets* is another component to be contemplated. It is important to consider whether the data is compared on a 1:1 or 1:n-basis. FRT used for identification purposes is 1:n matching and involves databases. The severity of the measure varies with the type of database used. If the datasets consist of lawfully collected police records, the intensity of the matching is less than when using databases based on images collected on a large scale from social media and the internet.[100] To address this, regulation should specify (and restrict) what lawfully collected sources may be used for matching.[101]

As a fourth factor, the *timing* of the analysis is important. It is necessary to differentiate real-time and ex-post processing. Real-time data matching (usually based on CCTV-infrastructure) inherently acts as a severe interference for a large number of people, as the faces of all persons passing through a specific area are captured, analysed biometrically, and instantaneously matched to a database, allowing for "live" surveillance.[102] If the monitored area is publicly accessible, the severity of the interference is particularly high, because it is nearly impossible to avoid the data processing.[103] Due to the high level of intrusion into individuals' privacy, real-time FRT requires the highest level of justification to be considered necessary in a democratic society.[104] Real-time FRT use requires legal bases that restrict in detail the spaces allowed to be monitored and conditions under which data can be processed. For use in criminal proceedings, this requires a restriction to particularly serious crimes for the investigation of which CCTV footage can be analysed in real-time to search for individuals on a watchlist. In contrast, ex-post FRT use depends on specific events (usually the

[84] EDPB (n 43) 41; Mobilio (n 1) 5 and 14.
[85] EDPB (n 43) 4.
[86] Mobilio (n 1) 16.
[87] For an overview of covert investigations Driton Muharremi 'Measures of concealed (secret) criminal investigation' (2015) 14 International Journal of Economic and Law 83.
[88] As required by Article 8 (2) LED.
[89] See e.g., Article R 40-26 of the French Code of Criminal Procedure or § 98c of the German Code of Criminal Procedure; see Theodore Christakis and Alexandre Lodie, 'The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations "Strictly Necessary" and Proportional' (2023) 3 European Review of Digital Administration & Law 159, 162.
[90] EDPB (n 43).
[91] Jasserand (n 9) 302 et seq.
[92] Article 10 LED.
[93] See Thomas Marquenie and Katherine Quezada-Tavárez, 'Data Protection Impact Assessments in Law Enforcement' <https://doi.org/10.1002/9781119834175.ch2> accessed 30 September 2024.
[94] Martyna Kusak, 'Quality of data sets that feed AI and big data applications for law enforcement' (2022) (23) ERA Forum 209.
[95] Kindt (n 61), 528.
[96] CJEU c-594/12 (n 59) para 54.
[97] Buolamwini and Gebru (n 27) 9.
[98] Miriam Buiten, 'Towards intelligent regulation of artificial intelligence' (2019) 10(1) European Journal of Risk Regulation 51.
[99] Kusak (n 94) 210.
[100] Raposo (n 7) 9; Rezende (n 32) 384.
[101] EDPB (n 43) 235.
[102] See Glukhin v. Russia (n 4) para 86.
[103] Solarova et al. (n 6) 632.
[104] Glukhin vs. Russia (n 4) para 86.

commission of a crime) that retrospectively trigger the analysis.[105] Ex-post uses are less invasive, as they are naturally restricted in their scope. However, they also involve the generation and matching of biometric data. Therefore, the legal basis must clearly state when authorities can employ FRT to identify individuals through ex-post analysis.[106] In that regard, some Member States provide general legislation in their domestic law for the ex-post analysis of data with regard to identification databases in criminal investigations,[107] but lack specific rules when these are allowed to be used for biometric facial recognition processes.

4.1.3. Data exploitation

Once data is analysed by FRT, the result is exploited to generate value for criminal investigations. The results consist of information (i.e., biometric templates and data about facial resemblances) whose use constitutes further processing. Subsequent exploitation of the data must therefore be considered within a regulatory framework. As the use of the information can be very diverse, regulation should mainly focus on: (1) the *authorities responsible* for using the information, (2) factors relevant to the *interpretation* of the results, (3) *durability* and *spread* of the use, and (4) if the exploitation is limited to the initial *purpose* of data collection or whether it can be changed or extended.

It is firstly necessary to determine the *responsible authorities* authorized to access the information, use the data, and act upon the results.[108] In that regard, it is also relevant whether data exploitation necessitates outsourcing to private parties. If data storage involves outsourcing to private service providers, this must be carefully considered, as it entails a risk of third-party-access to the data, particularly if the provider operates in a country outside the EU with less stringent data protection laws.[109]

Second, *interpretation* of the results must be considered in light of the accuracy of the system used and results generated. This requires prior engagement with the performance metrics of the system and specification of minimally acceptable thresholds that will guide the responsible authorities when interpreting the results.[110] Regulation should provide such guidelines for interpretation of the results. This also raises awareness that statistical procedures can be error-prone and are not free of discriminatory bias.

Third, the *durability* of the exploitation is relevant, and connected with that also its *spread*. It makes a difference whether the information generated is simply used once (and deleted afterwards) or retained in a database for recurring use. The storage and retention of data must be specifically provided for.[111] Among other reasons, this is important because the mere storage of citizens' personal data in governmental databases exposes this data to potential cyber-attacks.[112] In terms of the *spread* of use, it is important to consider whether exploitation makes the data accessible to additional persons, authorities, or institutions. Any disclosure of data to additional parties requires transparent rules regarding when the authorities can grant access and on what grounds.[113]

Lastly, it is necessary to consider the *purpose* for which the data is exploited. It is important to determine if the purpose corresponds with the original purpose for which the data were collected or generated (Article 4 (1) (b) LED). Every subsequent use for purposes other than the original one requires specific legal justification.[114] In that regard, it is relevant to consider whether the new purpose serves the provision of "positive" governmental services from which citizens may benefit (e.g., for identification in transportation services) or whether it is used for authoritative public intervention with possible sanctions for individuals. If the data is used for the former, the requirements would be lower. In any case, using data for a new purpose is only permissible if this is provided for in Union or Member State law (Article 4 (2) LED). Ultimately, the possibility of repeated or further use increases the intensity of the interference brought about by the use of FRT.

4.2. EU AI Act

The EU AI Act[115] is a general AI regulation on a European level which entered into force on 1 August 2024. The regulation is based on the competence of the Union regarding the functioning of the internal market (Article 114 TFEU) and data protection (Article 16 TFEU). The AI Act follows a risk-based approach. AI systems are regulated based on their risk for fundamental rights and safety.[116] This is done by classifying them into four categories: systems with unacceptable, high, limited, or minimal risk.

The rules of the AI Act distinguish between real-time and ex-post FRT. Real-time FRT use in publicly accessible spaces for the purposes of law enforcement is considered unacceptably risky and generally prohibited (Article 5 (1) (h) AI Act). However, there are three exceptions in which the use of real-time FRT is allowed: (1) For the targeted search for victims of abduction, human trafficking or sexual exploitation as well as for missing persons; (2) for the prevention of a specific, substantial and imminent threat to life or safety or a terrorist attack and (3) for the localization or identification of a person suspected of having committed serious offences listed in Annex II (e.g., terrorism, organized crime, sexual exploitation of children) (Article 5 (1) (h) AI Act). If strictly necessary for one of these three purposes, the use of real-time FRT can be allowed. In sum, the exceptions are far-reaching and enable the use of real-time FRT to prevent serious threats, to search for victims and missing persons as well as for the investigation of specific serious crimes.

If Member States want to make use of real-time FRT according to these three exceptions, they must issue national legislation authorizing the use thereof. The exceptional authorization of real-time FRT in national law requires temporal, geographic and personal limitations, a fundamental rights impact assessment and a registration of the system in a database (Article 5 (2) AI Act). Furthermore, each exceptional use of real-time FRT requires prior authorization by a judicial or independent administrative authority (Article 5 (3) AI Act). Member States have to provide the necessary legislation in their national law and include detailed rules for the judicial authorization procedure. Member States may also introduce more restrictive laws on real-time FRT (Article 5 (5) AI Act).

Thus, in principle, real-time FRT use for law enforcement purposes is prohibited, but Member States have the possibility of authorizing real-time use in their national law for the three exceptional purposes in law enforcement. The third exception enables repressive use for the investigation of serious crimes (listed in Annex II of the AI Act). It should be noted, however, that it is questionable whether the EU is even competent to specifically regulate real-time use of FRT in nationally conducted criminal investigations, as criminal proceedings generally

[105] Christakis and Lodie (n 89) 160.
[106] Christakis and Lodie (n 89) 160.
[107] Cf. Article R40-26 of the French Criminal Procedural Code or § 98c of the German Criminal Procedural Code.
[108] EDPB (n 43) 35.
[109] Further on the risk of third-party-access in the context of data storage see Ndukwe Ukeje, Jairo Gutierrez and Krassie Petrova 'Information security and privacy challenges of cloud computing for government adoption: a systematic review' (2024) 23 International Journal of Information Security 1459.
[110] EDPB (n 43) 33; see also Raposo (n 7) 13.
[111] Kindt (n 61) 527 f.
[112] Bernd Wirtz and Jan C. Weyerer, 'Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats' (2017) 40 (13) International Journal of Public Administration 1085.
[113] Council of Europe, 'Practical guide on the use of personal data in the police sector' (2018) <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> accessed 30 September 2024.
[114] Council of Europe (n 113) 4.
[115] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on Artificial Intelligence.
[116] Barkane (n 6) 152.

remain within the competence of Member States.[117]

Besides the (not so strict) prohibition of real-time FRT, the AI Act contains a second prohibition that affects FRT in law enforcement. According to Article 5 (1) (e) AI Act, the placing into the market, putting into service, or use of AI systems that create or expand facial recognition databases through the "untargeted scraping of facial images from the internet or CCTV footage" is prohibited. FRT systems that operate with databases based on indiscriminate web scraping methods that collect facial images online are illegal. For instance, the software Clearview AI would fall under this prohibition.

Apart from the described prohibited practices, the AI Act regulates high-risk AI systems by subjecting them to a set of mandatory requirements. Any AI system used for the biometric identification of natural persons is classified as high-risk (Article 6 (2) and Annex III (1) AI Act). It is required to implement a risk management system and data governance measures (including qualitative requirements for training, validation, and testing data and measures against biases), establish technical documentation and enable the automatic recording of events (Article 9–27 AI Act). These requirements apply for both ex-post and real-time FRT (if not already prohibited). Additionally, the AI Act introduces a specific obligation for ex-post use in criminal investigations: Ex-post use of FRT for the targeted search of a person convicted or suspected of having committed a criminal offence requires a judicial authorization for the use of that system in an investigation (Article 26 (10) AI Act). Also here, however, there is an exception: the requirement of judicial authorization does not apply if the ex-post system is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence (Article 26 (10) AI Act).

4.3. Appraisal

The AI Act's regulatory approach to FRT is worthy of evaluation, considering the procedural perspective introduced above. Overall, the rules follow a graduated risk approach based on two specific prohibitions and general requirements for biometric AI systems. Even though classifying AI systems which perform biometric analyses as high-risk or even prohibited recognizes the intensity of such analyses, the approach contrasts with the procedural understanding of technology use. The multiple interferences associated with FRT, which vary in degrees of invasiveness, are assessed in a general manner by the regulation and without considering the data processing steps. From that perspective, the AI Act is not a comprehensive regulatory framework for FRT use by law enforcement. The AI Act was intended as horizontal regulation of AI systems with elements of product safety and consumer protection, but also surveillance and fundamental rights protection.[118] Consequently, it is more of a general framework with overarching guidelines for AI. Still, the regulation establishes a set of rules for the use of biometric AI systems, and with that introduces a new approach to regulate FRT use. At the same time, much remains unregulated in terms of FRT in law enforcement, and these gaps must be filled by specific laws in Member States deploying FRT for law enforcement purposes. We will identify and discuss these gaps below.

Looking at the chain of value creation and exposure, it can be seen that beyond the prohibition of scraping images, data collection is not regulated in detail. What is needed is regulation of the type and source of data collected, categories of individuals affected, recognizability of the measure, and specific purpose of the collection. These aspects are not addressed in the provisions.[119]

For data analysis, the rules are more complex. Analysis by FRT is particularly sensitive, with several aspects to consider. It is necessary to address the risk of bias and ensure the quality of the datasets used. Here, the AI Act takes an important step by setting mandatory requirements and qualitative criteria for datasets used for high-risk AI systems.[120] In contrast, legal foundations for the generation of biometric data and matching of databases in the context of FRT are not provided. Regarding matching databases, the AI Act provides one rule: prohibition of databases built through untargeted scraping methods. However, it is not sufficient to prohibit certain types of databases. It is necessary to regulate what databases are allowed for use in matching.

The aspect of timing is well reflected in the AI Act, which distinguishes between real-time and ex-post FRT use. The regulation provides quite detailed rules for the application of real-time FRT: Generally prohibited, real-time use is exceptionally allowed for three specific purposes. Thus, the prohibition is by no means absolute but opens the door for both repressive and preventive purposes. The exceptions are quite far-reaching and grant Member States the possibility to opt-in for the exceptionally allowed real-time applications. It remains in the competence of the Member States to authorize real-time FRT use in their territory. Detailed national legislation, however, would be necessary which complements the rules set by the AI Act.

In contrast to the rules for real-time FRT, the AI Act only contains one rule for ex-post use in the context of criminal investigations, namely the requirement of a judicial authorization. Also here, there is an exception if the system is used for initial identification of a potential suspect and based on facts linked to the offence (e.g., analysis of CCTV footage capturing the suspect committing an offence), which might cover a large part of typical ex-post applications in criminal investigations. Notwithstanding this specific rule for ex-post identification, national legislation remains in any case necessary to authorize ex-post FRT use in criminal investigations.

Apart from regulating the concrete application of real-time and ex-post biometric identification systems, it would be necessary to provide technical, organizational, and procedural safeguards that accompany the biometric processing. Hereto, the AI Act sets mandatory requirements for the technical systems being used. Beyond the requirements of the AI Act, it is necessary to include organizational and procedural safeguards (i.e., sufficient guarantees against the risk of abuse and effective legal remedies for persons affected by the analysis).[121]

Finally, the AI Act does not contain rules regarding data exploitation. There are no rules specifying the responsible authorities, interpretation of results, or durability and spread of subsequent data exploitation.

In sum, the AI Act is not a comprehensive legal framework for FRT use in law enforcement. Because FRT comes with severe interferences, it is necessary to have clear and detailed legal bases governing its scope and application for law enforcement.[122] The provisions of the AI Act address single, specific, and (of course) important issues associated with AI-based biometric identification but they were not intended as legal bases for FRT use, but rather to set red lines for real-time FRT applications. Since the provisions cannot be invoked as legal bases, national rules are indispensable for authorities seeking to deploy the technology.[123] In that regard, national transpositions of the LED that generally regulate under which conditions biometric data is allowed to be processed (e.g., by general clauses referring to the requirements of strict necessity and appropriate safeguards) would not suffice as law authorizing FRT.[124] Specific legal bases are necessary that precisely foresee the biometric identification by means of FRT for clearly defined purposes.

[117] See the discussion in Ch. 4.3 on this issue.
[118] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 Computer Law Review International 97, 112.
[119] See also Raposo (n 7) 8 et seq.
[120] Mobilio (n 1) 22.
[121] EDPB (n 43) 17.
[122] Glukhin v. Russia (n 4) para 82.
[123] Mobilio (n 1) 19.
[124] EDPB (n 43) 21.

Detailed national legislation is all the more necessary as the EU only has limited competences in criminal procedural law.[125] This stands in contrast to the quite detailed rules for (exceptional) real-time FRT that would be expected in national criminal procedural codes, but not in an AI regulation based on the EU's internal market and data protection competence.[126] Criminal proceedings, particularly the collection, use and admissibility of evidence, including such based on technology like FRT, are generally regulated by national criminal procedural law.[127] If Member States intend to make use of FRT, their national legislation must contain clear rules and limitations governing its application in criminal proceedings.[128] The AI Act provides certain guidelines for this but does not constitute a stand-alone legal framework. Therefore, the use of FRT in law enforcement requires establishment of a legal framework beyond the AI Act. The approach developed here supports this endeavor.

5. Conclusion

The use of FRT is slowly but steadily spreading in criminal investigations across Europe. The technology bears great potential to support the investigation of crimes by enabling remote identification of individuals, based on a biometrical analysis of facial images and matching with a database. Due to the biometric nature of the analysis, the use of FRT in law enforcement is legally sensitive. Its use in criminal proceedings has severe implications for fundamental rights, thus necessitating appropriate regulation. The goal of the present contribution was to determine the legal implications of FRT use in law enforcement and assess regulatory cornerstones for criminal investigations.

Based on a procedural understanding, this analysis shed light on the complexity and severity of the whole facial recognition process. FRT constitutes multi-step data processing. Beginning with the collection of facial images, data are analyzed biometrically (implying the creation of data of a new quality) and matched against databases, resulting in information that is subsequently exploited. Each of these processing steps interferes with fundamental rights, and thus each step must be regulated appropriately.

Regarding data collection, a legal framework should address the type of data collected, sources of the data, categories of persons affected, recognizability of the processing, and its specific purpose. However, FRT regulation must go beyond the collection of facial images. That is the key point made by this contribution. The data analysis performed by FRT is particularly sensitive, as it generates biometric information. Due to this biometric nature, the data analysis is unique and accompanied by particularly severe interferences. The data generation and matching with databases must be recognizable for citizens, as should the conditions of the analysis itself. It must be clear in which specific scenarios the biometric analysis will take place, in real-time or ex-post. Moreover, technical, organizational, and procedural safeguards are required. Finally, a legal framework should consider subsequent exploitation of the data by determining what institutions dispose of the information, the spread and durability of the exploitation, interpretation of results, and specific use for which the data is exploited. Misuse can only be avoided through clear rules governing exploitation of the data.

The AI Act regulates AI systems used in the EU and establishes certain rules for the use of FRT. An evaluation of the regulation showed, however, that the provisions of the AI Act are not sufficiently clear and precise to serve as a legal framework for FRT use by law enforcement authorities of Member States. The AI Act rather serves as baseline framework, prohibiting specific applications of FRT and providing fundamental requirements for FRT systems in use. Similarly, national transpositions of the LED merely setting general requirements for the processing of biometric data cannot serve as legal bases for the biometric analysis. If Member States wish their law enforcement authorities to make use of FRT's potential, they must develop specific legal bases that precisely authorize the use of the technology in specific situations and provide legal bases for the collection, analysis and exploitation of data. The aspects compiled here can help to guide policymakers in developing such a comprehensive legal framework, if the application of FRT in law enforcement is deemed necessary. If a legal framework is not enacted, the use of FRT in criminal proceedings remains prohibited.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

[125] Schroeder (n 51) 145. The Union would have competencies to establish minimum rules for the approximation of law if this is necessary to facilitate the mutual recognition of judgements and judicial decisions as well as police and judicial co-operation in criminal matters with a cross-border dimension, e.g., regarding the mutual admissibility of evidence (Article 82 (2) (a) TFEU). Until now, the EU has not yet adopted legislative instruments on mutual admissibility of evidence. Thus, the collection, use and admissibility of evidence remain left to the laws of the national criminal procedure of the Member States, see Balázs Garamvölgyi et al. 'Admissibility of Evidence in Criminal Proceedings in the EU' (2021) 3 EuCrim 201, 202; Lorena Bachmaier, 'Mutual Admissibility of Evidence and Electronic Evidence in the EU' (2023) 2 EuCrim 223, 223.

[126] Valta and Vasel (n 51) 143; Martin Ebers et al., 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) J Multidisciplinary Scientific Journal 4, 589, 590.

[127] John Vervaele, 'Lawful and Fair Use of Evidence from a European Human Rights Perspective' in: Fabio Giuffrida and Katalin Ligeti (Eds.), Admissibility of OLAF final reports as evidence in criminal proceedings, 66 <https://orbilu.uni.lu/bitstream/10993/40141/1/ADCRIM_final_report.pdf > accessed 30 September 2024.

[128] Glukhin v. Russia (n 4) para 82.