9

Government Use of Facial Recognition Technologies under European Law

Simone Kuhlmann

State actors in Europe, in particular security authorities, are increasingly deploying biometric methods such as facial recognition for different purposes, especially in law enforcement, despite a lack of independent validation of the promised benefits to public safety and security. Although some rules such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) are in force, a concrete legal framework addressing the use of facial recognition technologies (FRTs) in the EU so far does not exist. Given the fact that the technology is processing extremely sensitive personal data, is not always working reliably, and is associated with risks of unfair discrimination, a general ban on any use of artificial intelligence (AI) for automated recognition of human features at least in publicly accessible spaces has been demanded.[1] Against this background, this chapter adopts a fundamental rights perspective and examines whether and to what extent government use of FRT can be accepted under European law.

9.1 GOVERNMENT USE OF FACIAL RECOGNITION TECHNOLOGIES WITHIN THE EU

The government use of FRT in the EU is limited so far. With Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Slovenia, and the Netherlands, eleven countries are already using FRT, with an upward trend, but the deployments are primarily experimental and localised so far.[2] It is mainly used by security authorities for the purposes of prevention, investigation, detection, and

[1] European Data Protection Board (EDPB), 'EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination', Press Release (21 June 2021), https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en; European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

[2] 'Biometric & behavioural mass surveillance in EU member states' (2021), Report for the Greens/EFA in the European Parliament, p. 36 et seq.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

prosecution of criminal offences as well as the prevention of threats to public security. In addition to the most controversial use of FRT for (mass) surveillance, especially in publicly accessible spaces, FRT is primarily used among law-enforcement agencies in the EU for the purposes of forensic authentication so far.[3] The typical scenario is to match the photograph of a suspect (e.g., extracted from previous records or closed-circuit television footage) against an existing database of known individuals (e.g., a national biometric database, a driver's licence database) for *ex-post* identification in a criminal investigation. Finally, on grounds of efficiency, FRT is also increasingly used by law enforcement agencies as a tool for analysing large amounts of video footage, for instance to search for a specific person or to track a person over multiple videos, since a manual analysis can be very time and resource consuming.[4]

9.2 SUITABILITY DESPITE ACCURACY CONCERNS

A ban on use of FRT for law enforcement purposes is still discussed under the recurring argument that the performance of such systems is not yet appropriate. The sufficient accuracy rates cannot be achieved in real life settings, the errors are unequally distributed in the referenced population, and minorities are discriminated against.[5]

If methods or systems are not reliable and mistakes occur when implementing the method or the system in practice, its use by state authorities may be unlawful. Under European law, the exercise of recognised rights and freedoms can be limited only if such limiting measures are appropriate and necessary to achieve the objectives (see Art. 52 para. 1 EU Charter of Fundamental Rights (CFR)). If this is lacking, the measures are disproportionate and thus unlawful. However, the European Court of Justice (CJEU) allows a wide margin of assessment to the legislator to assess the suitability of the measure. Only if, having regard to its objective, the measure is manifestly inappropriate, can the legality of a measure be affected. As long as the objective is promoted in any way, the measure is presumed to be appropriate, even if the employed method is not wholly reliable. Hence, the CJEU assessed the storage of biometric fingerprints in passports and travel documents for the purpose of preventing illegal entry to the EU as generally suitable, despite a not inconsiderable error rate.[6] The court came to the same conclusion with relation to the automated analysis of passenger name records (PNR) for the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime.[7] With regard to

[3] Ibid., p. 38.

[4] Stephan Schindler, 'Biometrische Videoüberwachung – Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung mit Videoüberwachung zur Bekämpfung von Straftaten' (2020), p. 211; Gerrit Hornung and Stephan Schindler, 'Das biometrische Auge der Polizei' (2017) 5 *ZD* 203.

[5] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

[6] CJEU, Case 291/12, *Michael Schwarz* v. *Stadt Bochum* [2013], ECLI:EU:C:2013:670, p. 43.

[7] CJEU, Case 817/19, *Ligue des droits humains* v. *Conseil des ministres* [2022], ECLI:EU:C:2022:491, pp. 123–124.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

the automated matching of PNR data with patterns, which is comparable in its functioning to facial recognition systems, the CJEU stated that the possibility of 'false negatives' and the fairly substantial number of 'false positives' resulting from the use of the system may limit the appropriateness of the system. However, automated processing has indeed already made it possible to identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime; this is why the system is not inappropriate.[8] Moreover, according to the CJEU, the appropriateness of the system essentially depends on the proper functioning of the subsequent verification of the results obtained under those processing operations by non-automated means.[9]

The FRT technologies have made real progress towards accuracy in the last years, owing to the use of convolutional neural networks. Despite this, the accuracy and error rates of FRT systems depend strongly on the task and the conditions under which the technology is used, as well as the quality of training and comparison data.[10] The one-to-one variant has become extremely accurate.[11] It is used to confirm a person's identity on the basis of clear reference images, such as recognising the rightful owner of a passport or smartphone (verification/authentication). On standard assessments such as the Facial Recognition Vendor Test (FRVT) of the National Institute of Standards and Technology (NIST), accuracy scores can be as high as 99.97 per cent.[12] This is, with some reductions in accuracy, true even if the face is partially covered by a mask.[13] The reason for this is that the one-to-one variant is comparatively simple. In one-to-one situations, one typically deals with standardised images often produced under ideal conditions (e.g., consistency in lighting and positioning), which correspondingly leads to a lower number of inaccuracies.

The situation is quite different if FRT is used in the one-to-many variant,[14] which receives most attention in the debate. This variant serves to determine an unknown person's identity by comparing a facial image with a large volume of known faces (identification). For example, it can be used to identify specific offenders or suspects or track down missing persons or victims of kidnapping.[15] Compared with the verification systems, the pictures of individuals used for identification purposes were usually captured remotely and in real life settings ('in the wild'), where the subjects

[8] Ibid., p. 123.

[9] Ibid., p. 124.

[10] Davide Castelvecch, 'Beating biometric bias' (2022) 587 *Nature* 348.

[11] Ibid., p. 349; William Crumpler, 'How accurate are facial recognition systems – And why does it matter?' (14 April 2020), Center for Strategic and International Studies, www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

[12] Crumpler, 'How accurate are facial recognition systems?'.

[13] Mei Ngan, Patrick Grother, and Kayee Hanaoka, 'Ongoing Face Recognition Vendor Test (FRVT), Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms' (November 2020), NISTIR 8331, https://doi.org/10.6028/NIST.IR.8331.

[14] Castelvecchi, 'Beating biometric bias', p. 349.

[15] For more examples see EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, p. 9.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

do not know they are being scanned. They may not be looking directly at the camera and/or may be obscured by objects or shadows. Accordingly, the accuracy rates tend to be far lower when compared with the controlled setting. For example, NIST's FRVT found that, when using footage of passengers entering through boarding gates (a relatively controlled setting), the best FRT system had an accuracy rate of 94.4 per cent.[16] In contrast, leading algorithms identifying individuals walking through a sporting venue – a much more challenging environment – had accuracies ranging between 36 per cent and 87 per cent, depending on camera placement.[17] These different uses with a broad range of accuracy could cause fundamental rights concerns.

9.3 FUNDAMENTAL RIGHTS CONCERNS

The government use of FRT interferes with the European fundamental right guarantees. First of all, the initial video recording, the subsequent retention of the footage, and the comparing of the footage with database records for the purpose of identification (matching) constitutes an interference with the right to data protection, as set out in Article 8 CFR and Article 16 Treaty on the Functioning of the European Union (TFEU).[18] Both regulations ensure identical protection of personal data against processing, including in particular the image of a person recorded or, rather, the unique facial features extracted in a template. In addition, the right to private life implemented in Article 7 CFR and Article 8 European Convention on Human Rights (ECHR) might also be violated, depending on how and for what purpose the technology is used. Article 7 CFR protects privacy to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.[19] The protection guaranteed by Article 7 CFR and Article 8 ECHR extends primarily to private zones (a person's home or private premises). However, there can also be interaction in a public context, which may fall within the scope of private life, when the person can have the reasonable expectation to be in private (e.g., private conversation in a screened area).[20] Such expectation cannot exist in a public space where everyone is visible to any member of the public.[21]

Accordingly, the use of FRT by authorities is not necessarily inconsistent with Article 7 CFR and the right to private life, as long as the video recording is made in

[16] Patrick Grother, George Quinn, and Mei Ngan, 'Face in Video Evaluation (FIVE): Face recognition of non-cooperative subjects' (March 2017), NISTIR 8173, https://doi.org/10.6028/NIST.IR.8173.

[17] Ibid.

[18] European Parliamentary Research Service (EPRS), 'Regulating facial recognition in the EU' (September 2021), p. 10.

[19] ECtHR, *Niemietz* v. *Germany*, judgment of 16 December 1992, Series A no. 251-B, pp. 33–34, § 29; *Botta* v. *Italy*, judgment of 24 February 1998, Reports of Judgments and Decisions 1998-I, p. 422, § 32.

[20] ECtHR, *P.G. and J.H.* v. *the United Kingdom*, no. 44787/98, § 56; *Peck* v. *the United Kingdom*, no. 44647/98, § 57.

[21] See ECtHR, *Uzun* v. *Germany*, judgment, no. 35623/05, § 44.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

a public space where one cannot expect to be in private and is used solely for the purpose of identification. This applies at least as long as the recording is not stored systematically and permanently.[22] If FRT is used to gain inferences about the person and their personality, for example, their behaviour, whereabouts, movement patterns, contacts, or personal characteristics such as sexual or political orientation, Article 7 CFR might be violated, as the respect of private life includes the protection of private information and free development of personality.[23]

Furthermore, depending on the task for which the technology is used, FRT may affect other fundamental rights. For instance, if authorities deploy facial recognition systems in the context of public protests, during the protest or *ex-post*,[24] to identify participants or locate individuals suspected of offending, interference with the freedom of assembly according to Article 12 CFR and Article 11 ECHR comes into consideration.[25] In addition, there might a violation of a person's freedom of opinion and expression as guaranteed by Article 11 CFR. Assemblies and protests are legally protected as spaces for the collective expression of opinions. The use of FRT and the consequent possibility of identification and traceability may discourage individuals from exercising their right to freedom of peaceful assembly as well as their right to freedom of expression.[26]

9.4 LAWFULNESS UNDER THE EUROPEAN RIGHTS FRAMEWORK

These interferences with European fundamental rights do not make the government use of FRT generally inadmissible. Fundamental rights enshrined in the CFR and, in particular, the rights of data protection and private life, are not absolute rights; they must be considered in relation to their function in society and can be limited under certain circumstances.

9.4.1 *Specific Legal Bases*

First of all, Article 52(1) CFR requires a specific legal basis for any limitations to fundamental rights.[27] Thus, the specific legal basis is required that authorises the

[22] Ibid.

[23] See ECtHR, *Niemietz* v. *Germany*, judgment of 16 December 1992, Series A no. 251-B, pp. 33–34, § 29; *Botta* v. *Italy*, judgment of 24 February 1998, Reports of Judgments and Decisions 1998-I, p. 422, § 32.

[24] For example, the police in Hamburg used FRT after the G20 summit in 2017 to identify offenders from private recordings and police videos as well as image and video material from S-Bahn stations and from the media.

[25] Schindler, 'Biometrische Videoüberwachung', p. 384.

[26] See 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020), Report of the United Nations High Commissioner for Human Rights.

[27] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, p. 13.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

deployment of FRT systems. The EU currently has no competence to comprehensively and conclusively regulate the powers of member states' public authorities to intervene in the processing of personal data.[28] It is therefore up to the member states to create regulations precisely describing the applications and the conditions for the use of FRT.[29] A recourse to the GDPR is not possible, as police data processing for the purpose of preventing and prosecuting criminal offences, which are as described earlier currently the main application field in the EU, is not covered by its scope (see Art. 2(2) lit. d GDPR).

When adopting a legal basis for the use of FRT in law enforcement, the member states must observe the general requirements of the LED.[30] It regulates the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences including the prevention of threats to public security. The LED imposes some restrictions on the processing of special categories of personal data such as biometric data. For instance, the Directive permits the processing and saving of biometric data for the purpose of uniquely identifying a natural person only where 'strictly necessary' and, *inter alia*, subject to appropriate safeguards for the rights and freedoms of the data subject (see Art. 10 LED). Automated decisions based on biometric data are completely prohibited unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place (see Art. 11(2) LED).

9.4.2 *Specific, Explicit, and Legitimate Purpose*

Secondly, according to Article 52(1) and the first sentence of Article 8(2) CFR, as well as the requirements of the LED, the legal basis must specify in detail the purposes for which facial biometric data may by processed and by whom.[31] It must lay down clear and precise rules governing the scope and application of the measure in question.[32] In particular, the conditions and circumstances in which authorities are empowered to resort to any measures of secret surveillance and collection of data must be sufficiently clearly defined.[33] The reason for this is twofold: On the

[28] Art. 16(2) TFEU only empowers the EU to adopt rules relating to the protection of individuals with regard to the processing of personal data by the member states when carrying out activities that fall within the scope of EU law and on the free movement of such data.

[29] Schindler, 'Biometrische Videoüberwachung', p. 404; see also Vera Lúcia Raposo, 'The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal'(2022) *European Journal on Criminal Policy and Research*, https://doi.org/10.1007/s10610-022-09512-y.

[30] See in detail EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, p. 17 ff.

[31] EDPB, Guidelines 05/2022, p. 13; EPRS, 'Regulating facial recognition in the EU', p. 14; Raposo, 'The use of facial recognition technology'.

[32] CJEU, Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, 54; Case 203/15 and 698/15, *Tele2 Sveringe AB* v. *Post- och telestyrelsen* [2016], ECLI:EU:C:2016:970, 109.

[33] ECtHR, *Shimovolos* v. *Russia*, no. 30194/09, § 68.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

one hand, it should be possible for a person affected to foresee the scope and the application of the measures in question. On the other hand, the legal basis should define and restrict the authorities' scope of action. General clauses that allow the processing of personal data for public interest purposes are, therefore, insufficient for the use of FRT. For instance, in a UK case, the Court of Appeal overturned a first instance decision and concluded that the legal framework – a Surveillance Camera Code – did not qualify as legal basis, because it was imprecise and afforded individual police officers too much discretion.[34] The court considered that it was not clear who could be placed on the watchlist, nor was it clear that there were any criteria for determining where FRT can be deployed.[35]

The specified purpose for which the data processing is authorised in the legal basis must, according to the second sentence of Article 52(1) CFR, genuinely meet the objectives of the general interest recognised by the EU or meet the need to protect the rights and freedoms of others.[36] The fight against crime in order to ensure public security, which is the main purpose of FRT in the EU so far, in principle constitutes such an objective of general interest according to the case-law of the CJEU,[37] as well as European law. In several passages in the European Treaties, the European legislator expresses the role of the EU as an 'area of freedom, security and justice' (see Art. 67(1) TFEU), in which the 'prevention and combating of crime' (see Art. 3(2) TEU, Art. 67(3) TFEU) constitutes an objective of general interest. The ECHR also recognises the legitimacy of such purposes. According to Article 8(2) ECHR, an interference by a public authority can *inter alia* be accepted in the 'interests of national security, public safety or the prevention of disorder or crime', which includes the detection of crimes that have already been committed.[38]

The purpose and extent to which the government use of FRT can be permitted under the European legal framework depends on the degree of interference with fundamental rights. Depending on the application and task, the deployment of FRT by authorities can affect these fundamental rights in different degrees. If authorities solely use the technology *ex post* to identify a person who committed a crime, and, for this purpose, match the image of the suspect against an existing database, the infringement of the fundamental rights is rather limited.[39] In this case, the conduct of the affected person causes the data processing, and the data used for matching are sometimes already available in the authorities' databases. The situation is quite different when FRT is used by safety authorities in publicly accessible spaces for the purpose of prevention, detection, and prosecution of crime, as well as for the detection of persons

[34] Judgement in Case No. C1/2019/2670, Court of Appeal, 11 August 2020, 90–96.

[35] Ibid.

[36] See EDPB, Guidelines 05/2022, p. 14.

[37] CJEU, Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, 42; see also Case C-145/09, *Land Baden-Württemberg* v. *Panagiotos Tsakouridis* [2010], EU:C:2010:708, 45–47.

[38] See ECtHR, *S. and Marper* v. *The United Kingdom*, nos. 30562/04 and 30566/04, 100.

[39] See Schindler, 'Biometrische Videoüberwachung', p. 613.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

of interest.[40] In this case, images are captured of the face of anyone who passes within the range of the camera, without a justification that their conduct might have a link, even an indirect or remote one, with crime and without any differentiation, limitation, or exception. Consequently, it can be described as a general, indiscriminate (mass) surveillance, where the interference with the fundamental rights and freedoms is wide ranging and must be considered to be particularly serious.[41] From a fundamental rights perspective, it must be considered that the deployment of FRT is generally more sensitive than conventional video surveillance. Unlike the latter, FRT is capable (for some applications in near real-time) to associate the footage with a specific person and the information already available about them, which enables the collection of further sensitive data and conclusions about the person's behaviour. In addition, an official announcement of the use of FRT in a certain area reduces the intensity of the infringement of fundamental rights but does not abrogate it.[42]

The extent of interference with fundamental rights caused by the deployment of FRT does not solely depend on the number of affected people, but also lies in the design of the system. If the recorded facial images from a public space are deleted automatically and immediately after the comparison with the database fails to find a match, the interference is not so severe.[43] However, if the authorities store the facial images including the information when and where the image was taken, systematically (e.g., in a biometric reference database) and for a longer period of time (e.g., to verify the identity of the affected person, hold it for later matching, or to draw inferences regarding behaviour or personality), then a considerable intrusive weight must be assumed. Further, the crucial factor is not only the length of data storage, but also the amount and type of data additionally collected when the facial image is taken. Finally, the secrecy of FRT use is also significant for the degree of interference, as it does not allow the person concerned to evade the technology or seek legal protection. This applies both for the deployment of FRT in certain areas and the storage of facial images (for instance from social media) in a reference database for later matching attempts.

9.4.3 *Lessons Learned from the Case Law Concerning Data Retention*

From the numerous CJEU decisions on data retention, such as those dealing with the storage of data for the purpose of the prevention and prosecution of serious crime arising in connection with the use of telecommunication services, we know

[40] Ibid., p. 608 et seq.

[41] See in this regard CJEU, Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, 57–65.

[42] Mario Martini, 'Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit' (2022), 1–2 *NVwZ-Extra* 6.

[43] See BVerfG, Urt. v. 18.12.2018, *Kfz-Kennzeichenkontrolle* 2, ECLI:DE:BVerfG:2018:rs20181218.1 bvr014215, 47–51.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

that the general preventive and indiscriminate retention of traffic and location data is not compatible with the fundamental rights under Articles 7, 8, and 11 CFR. This is the case even when such data retention is conducted for the purposes of combating serious crime, preventing serious threats to public security and equally safeguarding national security.[44] The CJEU considers the collection of data for these purposes to be permissible only if it is based on certain personnel, geographical, and temporal criteria, which limit the data processing to what is strictly necessary.[45] These limits may, in particular, be determined according to the categories of persons concerned. For instance, these activities may only target people whose data are likely to reveal a link with serious crime offences. Alternatively, they may be set by using a geographical criterion, where the competent national authorities consider that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for a commission of serious criminal offences.[46] According to the CJEU, those areas may include places with a high incidence of serious crime and places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure that regularly receive a very high volume of visitors, or strategic locations such as airports, stations, or tollbooth areas.[47]

Moreover, in one of its recent decisions on data retention, the CJEU has clarified that the processing of data relating to the civil identity of a user solely for the purpose of identifying the user concerned can be justified by the objective of preventing, investigating, detecting, and prosecuting criminal offences in general.[48] This is assuming that the data does not provide information other than that necessary for identification purposes, such as contact details of the user or information on the communication sent. Hence, if the data provides further information that allows precise conclusions concerning the private lives of the persons concerned, only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of such traffic or location data.[49]

Finally, according to the CJEU, there have to be minimum safeguards to ensure 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

[44] CJEU, Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, 51; Case 140/20, *G.D.* v. *Commissioner of An Garda Síochána* [2022], ECLI:EU:C:2022:258, 101.

[45] See CJEU, Case 511/18, 512/18 and 520/18, *La Quadrature du Net* v. *Premier minister* [2020], ECLI:EU:C:2020:791, 147; C-203/15 and C-698/15, *Tele2 Sverige AB* v. *Post- och telestyrelsen* [2016], EU:C:2016:970, 108.

[46] See CJEU, Case 511/18, 512/18 and 520/18, *La Quadrature du Net* v. *Premier minister* [2020], ECLI:EU:C:2020:791, 148–150; Case-203/15 and C-698/15, *Tele2 Sverige AB* v. *Post- och telestyrelsen* [2016], EU:C:2016:970, 111.

[47] See CJEU, Case 511/18, 512/18 and 520/18, *La Quadrature du Net* v. *Premier minister* [2020], ECLI:EU:C:2020:791, 150.

[48] Ibid., paras. 158–159; Case 746/18, *H.K.* v. *Prokuratuur* [2021], ECLI:EU:C:2021:152, 34.

[49] CJEU, Case 746/18, *H.K.* v. *Prokuratuur* [2021], ECLI:EU:C:2021:152, 35.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

access and use of that data.[50] The need for such safeguards is greater when personal data is subject to automatic processing and when there is a significant risk of unlawful access to the data.[51] Therefore, in addition to technical and organisational measures to ensure the protection and security of the data and their full integrity and confidentiality, there is a need for substantive and procedural rules that regulate the access to the data and to their subsequent use by authorities.[52] The legal rules that authorise the data processing, must restrict the purposes for which authorities are allowed to use the data to what is strictly necessary. The accepted safeguard against the risks of automatic processing is, apparently also from the CJEU, the individual review of the results by non-automated means, often called 'human in the loop'.[53] It should only be noted in passing since this kind of safeguarding is a dubious idea for many reasons, especially while there is so much literature and studies on deficits in human decision-making.

9.5 CONSEQUENCES FOR THE GOVERNMENT USE OF FRT

When trying to adopt these guidelines given by the European fundamental rights framework and the associated case-law concerning data retention in the use of FRT, it must be considered that facial recognition systems process data of similar or even higher sensitivity than traffic or location data. The processing of facial biometric data does not only enable the identification and verification of individuals. The systematic collection and evaluation of such data might – as described earlier – lead to conclusions about persons' behaviour and whereabouts; apart from the fact that increasing attempts are being made to draw inferences about individual personal attributes from facial appearance, such as sexual or political orientation or violent tendencies.[54] However, the face is a highly personal feature that cannot simply be amended, given that FRT even works if the face is partially covered.[55] Accordingly, the existing rules addressing the processing of biometric data – the GDPR and LED – impose particularly high requirements on the processing of such data and only permit it for the prevention of threats to high-priority legal interests, including the prosecution of serious criminal offences.

The analysis shows that, despite the interference with fundamental rights such as privacy or data protection as well as possible high error rates, the European

[50] CJEU, Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, para. 54; Case 746/18, *H.K.* v. *Prokuratuur* [2021], ECLI:EU:C:2021:152, 48.

[51] Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, para. 55; Case 511/18, 512/18 and 520/18, *La Quadrature du Net* v. *Premier minister* [2020], ECLI:EU:C:2020:791, 132.

[52] See Case 293/12 and 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* [2014], ECLI:EU:C:2014:238, 61–66.

[53] Case 817/19, *Ligue des droits humains* v. *Conseil des ministres* [2022], ECLI:EU:C:2022:491, para. 203.

[54] See Michael Kosinki, 'Facial recognition technology can expose political orientation from naturalistic facial images' (2021) 11 *Scientific Reports* 100, https://doi.org/10.1038/s41598-020-79310-1.

[55] See Ngan, Grother, and Hanaoka, 'Face recognition accuracy with face masks'.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

fundamental rights framework does not preclude government deployment of FRT in principle. However, a specific legal basis is required, defining clearly and precisely the purposes for which and by whom FRT can be used, who has access to the generated data, and how to proceed with the data once collected (e.g., retention and deletion periods). The law must not only consider the various applications and sectors where FRT can be used, but also address the different phases of the use, including the creation of a reference dataset and its deployment.[56] Furthermore, safeguards against abuse and any external (unauthorised) use are needed as well.

A government use of FRT for general preventive and indiscriminate mass surveillance purposes, in which individuals are recorded without a reasonable suspicion, would not be compatible with the European fundamental rights framework. In particular, establishing a state-owned biometric reference database with face images of persons without any specific reason (e.g., in order to be able to easily identify individuals in the future), would be contrary to fundamental rights. It would be nothing else but general and indiscriminate data retention. Hence, only individuals who have given the authorities a reason to do so, because they are dangerous or are suspected of having committed a crime, for example, may be recorded in the reference database. A deployment of FRT in publicly accessible spaces can only be allowed if it serves to avert threats to high-priority legal interests or to prosecute serious criminal offences. Such deployment should be geographically limited to high-risk areas or to areas with high probability of locating wanted persons.[57] This is likely to apply even if the facial image is deleted automatically and immediately after the comparison with the database is completed and no matches are found. The use of FRT systems is therefore conceivable, for instance, when tracking terrorists or serious criminals in highly frequented areas or strategic locations, such as airports, stations, or tollbooth areas. It could also be used for the surveillance of events or places where the risk of serious criminal offences is high. Moreover, the deployment of FRT may also be compatible with fundamental rights if it is used for *ex-post* identification of criminals, terrorists, or other persons of interest, or as a tool for the effective image and video evaluation (e.g., to recognise or track individuals in a video recording). Most importantly, the decisive factor for using FRT, which complies with fundamental rights, is that the incoming data should not be stored longer than necessary for the intended purposes and cannot be used for other purposes.

9.6 CONCLUSION

The analysis here leads to the conclusion that the government use of FRT can be permissible under the European fundamental rights framework if subjected to

[56] See Council of Europe, ‘Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Convention 108’ (28 January 2021), Guidelines on facial recognition, p. 8.

[57] A limitation to categories of persons is not technically possible when deployed in public spaces.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press

specific and strict conditions. In order to allow FRT use, a legislator should provide a specific legal basis regulating the deployment of FRT that is compatible with fundamental rights. In light of this, the EU AI-Act,[58] which provides general limitations to FRT use,[59] will not be sufficient as a legal basis, especially for the present main application of FRT by authorities: the prevention and prosecution of crime. There should be a legal basis directly legislated by the member states,[60] as the protection of national security as well as law enforcement fall under the legislative competence of the states and not the EU. In addition, an empirical study of the real effectiveness of FRT would be sensible and desirable considering the fundamental rights violations before widespread use. So far, the advocates of this technology have failed to provide enough evidence to prove that this technology can genuinely ensure public safety and security.

[58] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence and amending certain Union Legislative Acts, COM (2021) 206 final.

[59] The AI-Act only contains limitations for the use of real-time remote biometric identification systems deployed in publicity accessible space for the purpose of law enforcement (see Art. 5(1) lit. d of the Commission's AI-Act Proposal). However, the Commission's original AI-Act Proposal is silent regarding other modalities of FRT for law enforcement purposes, such as when this technology does not take place in real-time or it is not performed in public spaces. Only the proposals made by the European Parliament address these deployment modalities of FRT, see European Parliament, P9_TA(2023)0236.

[60] Recognised by Art. 5(4) of the AI-Act Proposal.

https://doi.org/10.1017/9781009321211.012 Published online by Cambridge University Press