FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS
A REALITY FOR EVERYONE IN THE EUROPEAN UNION

Facial recognition technology: fundamental rights considerations in the context of law enforcement

FRA Focus

Facial recognition technology (FRT) makes it possible to compare digital facial images to determine whether they are of the same person. Comparing footage obtained from video cameras (CCTV) with images in databases is referred to as 'live facial recognition technology'. Examples of national law enforcement authorities in the EU using such technology are sparse – but several are testing its potential. This paper therefore looks at the fundamental rights implications of relying on live FRT, focusing on its use for law enforcement and border-management purposes.

EU law recognises as 'sensitive data' people's facial images, which are a form of biometric data. But such images are also quite easy to capture in public places. Although the accuracy of matches is improving, the risk of errors remains real – particularly for certain minority groups. Moreover, people whose images are captured and processed might not know this is happening – and so cannot challenge possible misuses. The paper outlines and analyses these and other fundamental rights challenges that are triggered when public authorities deploy live FRT for law enforcement purposes. It also briefly presents steps to take to help avoid rights violations.

Contents

1. Facial recognition technology and fundamental rights: setting the scene

This focus paper explores fundamental rights implications that should be taken into account when developing, deploying, using and regulating facial recognition technologies. It draws on recent analyses and data (Section 3 and Section 4) and evidence from interviews conducted with experts and representatives of national authorities who are testing facial recognition technologies (Section 5).[1] The last sections (Section 6 and Section 7) provide a brief legal analysis summarising applicable European Union (EU) and Council of Europe law.

The paper forms part of FRA's larger research project on artificial intelligence, big data and fundamental rights.[2] It is the first paper to focus on the uses of facial recognition technology, and builds on the agency's extensive past work on the fundamental rights implications of the use of biometric data in large-scale EU information systems in the field of migration, asylum and borders.[3]

Facial recognition technology (FRT) allows the automatic identification of an individual by matching two or more faces from digital images. It does this by detecting and measuring various facial features, extracting these from the image and, in a second step, comparing them with features taken from other faces.[4]

In the private sector, facial recognition technology is widely used for advertisement, marketing and other purposes, with individual customers profiled and identified to predict their preferences towards products based on their facial expressions.[5] Other examples from the private sector include a football club using it in their stadium to identify people who have been banned from attending the club's matches;[6] using facial recognition technology to analyse facial expressions of job candidates in interviews;[7] and major internet and social media companies, such as Facebook, deploying facial recognition technologies to improve their systems, by tagging faces.[8]

The recent evolution of artificial intelligence (AI) powered facial recognition technology is not attractive only to the private sector. It also opens new possibilities for public administration, including law enforcement and border management. A considerable increase in accuracy achieved in the past few years has prompted many public authorities and private businesses to start using, testing or planning the use of facial recognition technologies across the world.

This, in turn, has sparked an intense debate on its potential impact on fundamental rights. For example, the large-scale use of facial recognition technology in combination with surveillance cameras in the People's Republic of China has led to many discussions and concerns about potential human rights violations, particularly with respect to detecting members of certain ethnic minorities.[9] Following an increased use of facial recognition in the US, a national survey published in September 2019 by the Pew Research Centre finds that, while slightly more than every second American (56 %) trusts law enforcement agencies to use these technologies responsibly, smaller shares of the public say they

1 FRA carried out eleven interviews between March and May 2019, in EU Member States such as Germany, France and the United Kingdom, to gain better insight into current testing, and the potential use, of facial recognition technology.

2 The following have been published so far as part of the research project: FRA (2018), *#BigData: Discrimination in data-supported decision making*, Luxembourg, Publications Office, May 2018; FRA (2019), *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights,* Luxembourg, Publications Office, June 2019. For more on the project, consult FRA's webpage on the project.

3 See, for example, FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018; FRA (2018), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018.

4 For more detail on how facial recognition technology works, see e.g. Introna, L. and Nissenbaum, H. (2010), *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030.

5 See for example: Italy, *Garante per la protezione dei dati personali, Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria*, 21 December 2017.

6 See EDRi, "Danish DPA approves Automated Facial Recognition", 19 June 2019.

7 See The Telegraph, "AI used for first time in job interviews in UK to find best applicants", 27 September 2019.

8 See Wired, "Facebook can now find your face, even when it's not tagged", 19 December 2017.

9 Human Rights Council (2019), *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, A/HRC/41/35; New York Times, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", 14 April 2019.

have such trust in technology companies (36 %) or advertisers (18 %).[10]

In a number of European countries, facial recognition technologies are being tested or used in different contexts in both private and public spheres. This paper examines a specific aspect: comparing footage obtained from video cameras (CCTV) against databases of facial images (e.g. a watchlist) for law-enforcement and border-management purposes. Often referred to as 'live facial recognition technology', it is a specific form of video surveillance – and analyses of its fundamental rights implications are lacking.

To date, there are few examples of national law enforcement authorities using live facial recognition technology in Europe.

Defining law enforcement authorities

The term 'law enforcement authorities' refers to Member State agencies and encompass "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

Source: Law Enforcement Directive, Article 1 (1)

The United Kingdom has tested facial recognition technology to identify people in real time by using street cameras. Other European Union (EU) Member States have engaged in testing and made plans for using facial recognition technology. For example, in Hungary, a project called *'Szitakötő'* (dragonfly) plans to deploy 35,000 cameras with facial recognition capabilities in Budapest and across the country. The cameras will capture drivers' license plates and facial images for maintaining public order, including road safety.[11] The Czech government has approved a plan to expand the use of facial recognition cameras – from 100 to 145 – at the Prague International Airport.[12] Police in Germany and France have carried out extensive testing. Sweden's data protection authority has recently authorised the use of facial recognition technology by the police to help identify criminal suspects, which allows the police to compare facial images from CCTV footage to a watchlist containing over 40,000 pictures.[13]

The processing of facial images is expected to be introduced more systematically in large-scale EU-level IT systems used for asylum, migration and security purposes.[14] As outlined in Section 5, most of these EU-wide systems will process facial images in the future, once the necessary legal and technical steps are completed. These images will be taken in controlled environments – for example, at police stations or border-crossing points, where the quality of the images is higher compared to that of CCTV cameras. FRA has already pointed to the fundamental rights risks of processing facial images in such IT systems in earlier publications.[15]

Despite the strong push from private industry and other stakeholders to use facial recognition technology, strong opposition has emerged, citing weaknesses. This led, for example, the world's largest corporate supplier of police body cameras (Axon) to announce this year that it would not deploy facial recognition technology in any of its products – because it was too unreliable for law enforcement work and "could exacerbate existing inequities in policing, for example by penalising black or LGBTQ communities".[16] In a similar vein, the city of San Francisco in the United States, among other cities, has banned the use of the technology because of its excessively intrusive nature into people's privacy and to avoid possible abuse by law enforcement agencies.[17]

Against this backdrop, a number of questions arise from a fundamental rights perspective: is this technology appropriate for law enforcement and border management use – for example, when it is used to identify people who are wanted by law

10 Pew Research Center (2019), "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly".

11 See e.g. at Hungary Today, "CCTV: Is it Big Brother or the Eye of Providence?", 18 January 2019. For the multiple legal – primarily data protection-related – concerns raised by the Hungarian Data Protection Authority in connection with this project, see the letter available on the Authority's website.

12 See Biometriupdate.com, "Expanded use of facial recognition at Prague international airport approved", 10 March 2019.

13 See e.g. Datainspektionen, "*Polisen får använda ansiktsigenkänning för att utreda brott*", 24 October 2019 and NewEurope, "Sweden authorises the use of facial recognition technology by the police", 28 October 2019.

14 For more information, see Table 2.

15 FRA (2018), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, FRA Opinion 1/2018 [Interoperability]*, Vienna, 11 April 2018; FRA (2018), *The revised Visa Information System and its fundamental rights implication – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion 2/2018 [VIS], Vienna, 30 August 2018; FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018; FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, June 2017.

16 Crawford, K. (2019), "Regulate facial-recognition technology", Nature 572 (2019), 29 August 2019, p. 565.

17 New York Times, "San Francisco Bans Facial Recognition Technology", 14 May 2019.

enforcement? Which fundamental rights are most affected when this technology is deployed – and what measures should public authorities take to guarantee that these rights are not violated?

The risk of errors in matching faces is the most frequently raised fundamental rights concern. However, fundamental rights concerns also stem from the weak position of the individuals whose facial images are captured and processed. Fundamental rights affected include, among others, human dignity, the right to respect for private life, the protection of personal data, non-discrimination, the rights of the child and the elderly, the rights of people with disabilities, the freedom of assembly and association, the freedom of expression, the right to good administration, and the right to an effective remedy and to a fair trial.

For example, facial recognition technology has higher error rates when used on women and people of colour, producing biased results, which can ultimately result in discrimination. The use of facial recognition technology can also have a negative impact on the freedom of assembly, if people fear that facial recognition technology is being used to identify them ("chilling effect").

Moreover, there are possible long-term implications, which are not within the scope of this focus paper. Curtailing privacy by processing large amounts of personal data, including in particular individual faces, may ultimately affect the functioning of democracy, since privacy is a core value inherent to a liberal democratic and pluralist society, and a cornerstone for the enjoyment of fundamental rights.

Civil society and private companies have advocated for a clear regulatory framework of facial recognition technology.[18] Furthermore, the European Commission's High-Level Expert Group on Artificial Intelligence (HLEG AI) specifically recommends the proportionate use of facial recognition technology and suggests that its application must be clearly warranted in existing laws,[19] given its growth fuelled by the increasing use of artificial intelligence. Case law is still virtually non-existent, with one recent exception adjudicated in the United Kingdom (judgment not final).[20]

18 See, for example, Big Brother Watch, Face Off Campaign, May 2019; Microsoft, Facial recognition: It's time for action, 6 December 2018. Big Brother Watch, supported by several UK Members of the Parliament and 25 rights, race equality and technology organisations as well as technology academics, experts and lawyers, published a "Joint statement on police and private company use of facial recognition surveillance in the UK" in September 2019.

19 European Commission, Independent High-Level Expert Group on Artificial Intelligence (2019), *Ethics guidelines for Trustworthy on AI*, April 2019, pp. 33-34.

20 UK, High Court of Justice (Queens' Bench Division – Divisional Court Cardiff), *The Queen (OTAO) Bridges and Chief Constable of South Wales Police and others*, [2019] EWCH 2341 (Admin), 4 September 2019.

2. Facial images as a unique biometric identifier in EU law

People's facial images constitute biometric data: they are more or less unique, cannot be changed, and cannot easily be hidden. Facial images are also easy to capture: in contrast to other biometric identifiers, such as fingerprints or DNA, a person is typically unable to avoid having their facial image captured and monitored in public.

EU law regulates the processing of facial images under the EU data protection acquis. Table 1 provides an overview of relevant EU data protection instruments, their subject matter, and whether they govern the processing of facial images as biometric data. In the field of police and judicial cooperation in criminal matters, the Law Enforcement Directive (Directive (EU) 2016/680)[21] is the most relevant instrument. It establishes a comprehensive system of personal data protection in the context of law enforcement.[22] The Law Enforcement Directive specifically refers to facial images as 'biometric data' when used for biometric matching for the purposes of the unique identification or authentication of a natural person.[23] The sectorial EU instruments governing large-scale EU information systems in the field of migration and security, listed in Table 2 in Section 5.2, complement the EU data protection *acquis*.

Biometric data is defined 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 [fingerprint] data."[24] EU data protection law recognises two categories of information as biometric data: 1) 'physical/physiological characteristics', which pertain to bodily characteristics such as facial features, fingerprints, retina and iris characteristics; and 2) 'behavioural characteristics', like deeply ingrained habits, actions, personality traits, addictions, etc.[25] This includes behavioural characteristics that could permit the unique identification of a person, such as a hand-written signature, or a way of walking or moving. Digital facial images belong to the first category.

Recital (51) of the GDPR makes a distinction between the legal nature of simple 'photographs' and biometric 'facial images'. The definition of biometric data applies to photographs only when these are processed through specific technical means allowing the unique identification or authentication of a natural person.[26]

'Special categories' of personal data

"[P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Source: Law Enforcement Directive, Article 10 (1); GDPR, Article 9 (1) and Regulation (EU) 2018/1725, Article 10 (1)

Due to their sensitive nature, facial images fall into the 'special categories of personal data' or sensitive data. As such, EU data protection law provides for enhanced protection, and additional safeguards, compared to other personal data.[27]

21 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89 (Law Enforcement Directive), OJ L 119, 4.5.2016, pp. 89-131.
GDPR, recital (41).

22 For more, see FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition, Luxembourg*, Publications Office, June 2018, pp. 31-33 and Chapter 8.

23 Law Enforcement Directive, Art. 3 (13). See also Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88 (GDPR), Art. 4 (14) as well as Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No. 1247/2002/EC (PE/31/2018/REV/1), OJ L 295, 21.11.2018, pp. 39-98, Art. 3 (18).

24 Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

25 Article 29 Data Protection Working Party (2012), *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN, WP193, Brussels, 27 April 2012, p. 4; Misra, P. (2018), 'Here's how face recognition tech can be GDPR compliant', thenextweb.com, 29 October 2018.

26 GDPR, recital (51); See also Regulation (EU) 2018/1725, recital (29).

27 For more, see FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition*, Luxembourg, Publications Office, June 2018.

Table 1: EU law instruments on data protection: provisions on facial images and their applicability

EU legal instrument on data protection	Definition of 'biometric data' (including 'facial image')	Personal scope	Material scope
Law Enforcement Directive (Dir. (EU) 2016/680)	Yes (Art. 3 (13))	EU Member States' law enforcement authorities	Automated processing of personal data in Schengen Member States and processing of personal data by any other means which form part of a filing system for the prevention, investigation, detection or prosecution of criminal offences – within the scope of EU law
General Data Protection Regulation (Reg. (EU) 2016/679)	Yes (Art. 4 (14))	All private actors established and public institutions operating in the EU as well as controllers and processors not established in the EU that offer goods/ services to data subjects in the EU	Automated processing of personal data in the European Economic Area and processing of personal data by any other means which form part of a filing system – within the scope of EU law (e.g. GDPR not applicable to national security-related data processing)
Data Protection Regulation for EU institutions, bodies and agencies (Reg. (EU) 2018/1725)	Yes (Art. 3 (18))	EU institutions, bodies and agencies	Personal data processing by EU institutions, bodies and agencies
Directive on privacy and electronic communications (Dir. 2002/58/EC, as amended by Dir. 2009/136/EC)	No	Any individual whose personal data are processed in the electronic communication sector in the EU (e.g. via internet and mobile/landline telephony and via their accompanying networks)	Transmission of data through public electronic communication services – except for activities falling outside the scope of EU law and activities concerning public security, defence, State security and the activities of the State in criminal law

Source: FRA, 2019 (based on EU law instruments listed in the table)

3. What is facial recognition technology?

Facial recognition technologies are biometric systems that allow the automatic identification and matching of a person's face. The technology extracts and further processes biometric data by creating a 'biometric template'.[28] For facial images, a biometric template detects and measures various facial features.[29]

Facial recognition

Facial recognition is the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals".

Source: Article 29 Data Protection Working Party (2012), Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 March 2012, p. 2

Facial recognition refers to a multitude of technologies that can perform different tasks for different purposes. In this regard, a key distinction is whether facial recognition is used for verification, identification or categorisation. Verification and identification deal with matching unique characteristics of individuals to determine their individual identity. Categorisation deals with deducing whether an individual belongs to a specific group based on his or her biometric characteristics – for example, sex, age, or race.

In the past few years, facial recognition technologies have strongly benefitted from increased data availability, computing power and the development of sophisticated machine learning algorithms.

3.1. Verification (one-to-one comparison)

Verification or authentication is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual.[30] Two biometric templates are compared to determine if the person shown on the two images is the same person. Such a procedure is, for example, used at Automated Border Control (ABC) gates used for border checks at airports. A person scans his or her passport image and a live image is taken on the spot. The facial recognition technology compares the two facial images and if the likelihood that the two images show the same person is above a certain threshold, the identity is verified. Verification does not demand that the biometric features be deposited in a central database. They may be stored, for example, on a card or in an identity/travel document of an individual.

3.2. Identification (one-to-many comparison)

Identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there. The facial recognition technology returns a score for each comparison indicating the likelihood that two images refer to the same person. Sometimes images are checked against databases, where it is known that the reference person is in the database (closed-set identification), and sometimes, where this is not known (open-set identification). The latter operation would be applied when persons are checked against watchlists. Using facial recognition technology for identification is sometimes referred to as Automated Facial Recognition (AFR).[31]

Identification can be used based on facial images obtained from video cameras. For this purpose, the system first needs to detect if there is a face on the video footage. Smart phone users might know

28 Article 29 Data Protection Working Party (2012), *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN, WP193, Brussels, 27 April 2012.

29 'Biometric template' means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications (see Art. 4 (12) of Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, pp. 85-135).

30 See also Kindt, E. (2013), Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis (1st edn. Springer, Governance and Technology Series 12, 2013) and Iglezakis, I. (2013), *EU Data protection legislation and case-law with regard to biometric application*, Aristotle University of Thessaloniki, 18 June 2013.

31 For example in Davies, B., Innes, M., and Dawson, A. (2018), *An Evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018.

when taking pictures that sometimes the camera automatically draws rectangles over faces.

Faces on video footage are extracted and then compared against the facial images in the reference database to identify whether the person on the video footage is in the database of images (e.g. on the watchlist). Such systems are referred to as Live Facial Recognition Technology (LFRT).[32] The quality of the facial images extracted from video cameras cannot be controlled: light, distance and position of the person captured on the video footage limit the facial features. Therefore, live facial recognition technologies are more likely to result in false matches as compared to facial images taken in a controlled environment, such as a border crossing point or a police station.

3.3. Categorisation (matching general characteristics)

Apart from verification and identification, facial recognition technology is also used to extract information about an individual's characteristics. This is sometimes referred to as 'face analysis'. It can, therefore, also be used for profiling individuals, which involves categorising individuals based on their personal characteristics.[33] Characteristics commonly predicted from facial images are sex, age and ethnic origin. Categorisation means that the technology is not used to identify or match individuals, but only characteristics of individuals, which do not necessarily allow for identification. However, if several characteristics are inferred from a face, and potentially linked to other data (e.g. location data), it could *de facto* enable the identification of an individual.

The use of facial recognition technology does not stop here. Researchers and companies have experimented with inferring other characteristics from facial images, such as sexual orientation.[34] Such tests are highly controversial from an ethics perspective. Facial recognition technology can also be used to infer emotions, such as anger, fear or happiness, and to detect whether people are lying or telling the truth. The latter was researched at selected EU external borders (Greece, Hungary and Latvia) in the framework of the Integrated Portable Control System (iBorderCtrl) project, which integrates facial recognition and other technologies to detect if a person is saying the truth.[35]

The serious fundamental rights implications of the categorisation of individuals based on facial images is beyond the scope of this paper, which focuses on the use of facial recognition technology for identification purposes.

32 Fussey, P. and Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex, Human Rights Centre, July 2019.

33 See FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018.

34 Wang, Y. and Kosinski, M. (2018), 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images', *Journal of Personality and Social Psychology*, 114(2), pp. 246-257.

35 See European Commission, "Smart lie-detection system to tighten EU's busy borders," 24 October 2018, and the website of iBorderCtrl.

4. Accuracy of facial recognition technology: assessing the risks of wrong identification

4.1. Technological developments and performance assessment

The high level of attention given to facial recognition technology in the recent past stems from strong accuracy gains achieved since 2014.[36] The accuracy gains are mainly attributed to the availability of increased computational power, massive amounts of data (digital images of people and their faces), and the use of modern machine learning algorithms.[37]

Determining the necessary level of accuracy of facial recognition software is challenging: there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01 %) still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others, as described in Section 3. There are different ways to calculate and interpret error rates, so caution is required.[38] In addition, when it comes to accuracy and errors, questions in relation to how easily a system can be tricked by, for example, fake face images (called 'spoofing') are important particularly for law enforcement purposes.[39]

Facial recognition technologies, like other machine-learning algorithms, have binary outcomes, meaning that there are two possible outcomes. It is therefore useful to distinguish between false positives and false negatives:

- A 'false positive' refers to the situation where an image is falsely matched to another image on the watchlist. In the law enforcement context, this would mean that a person is wrongly identified as being on the watchlist by the system. This has crucial consequences on that persons' fundamental rights. The "false positive identification rate" gives the proportion of erroneously found matches (e.g. number of people on the watchlist identified who are in fact not on the watchlist) among all those who are not on the watchlist.

- False negatives are those who are deemed not to be matches (i.e. not on the watchlist), but in fact are matches. The corresponding "false negative identification rate", or "miss rate", indicates the proportion of those erroneously not identified among those who should be identified.

The issue of false positives and false negatives is also connected to data quality and to the accuracy of data processing. Addressing this requires a regular correction and updating of the facial images stored in a watchlist in order to ensure accurate processing.

When discussing error rates, three important considerations need to be kept in mind:

- First, an algorithm never returns a definitive result, but only probabilities. For example: with 80 % likelihood, the person shown on one image is the person on another image on the watchlist. This means that thresholds or rank-lists need to be defined for making decisions about matches.

- Second, as a consequence, there is always a trade-off between false positives and false negatives because of the decision on a probability threshold. If the threshold is higher, false positives will decrease, but false negatives will increase, and the other way round. This is why such rates are usually reported with the other rate at a fixed level (e.g. the miss rate is reported at the fixed false positive identification rate of 0.01, i.e. 1 %).[40]

- Third, the rates need to be evaluated with the quantities of real cases in mind. If a large number of people are checked in mass, a potentially small false positive identification rate still means that a

36 See Grother, P., Ngan, M., and Hanaoka, K. (2018), Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238; or Galbally, J., Ferrara, P., Haraksim, R., Psyllos, Al, and Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Luxembourg, Publications Office, July 2019.

37 For facial image recognition, the success mostly stems from the use of deep convolutional neural networks. These algorithms learn generic patterns of images by splitting images in several areas.

38 For more detailed discussions of evaluation metrics, see Grother, P., Ngan, M., and Hanaoka, K. (2018), Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238; or Galbally, J., Ferrara, P., Haraksim, R., Psyllos, Al, and Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System, Luxembourg*, Publications Office, July 2019.

39 See for example: Parkin, A. and Grinchuk O. (2019), Recognizing Multi-Modal Face Spoofing with Face Recognition Networks.

40 E.g. Grother, P., Ngan, M., and Hanaoka, K. (2018), Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238.

significant number of people are incorrectly identified. For example, a false positive identification rate of 0.01 means that among 100,000 people, 1,000 will be erroneously flagged. The assessments of accuracy are usually done on the basis of specified training data sets and cannot easily be evaluated when deployed. One of the reasons is that those missed in a real world scenario are not known.

Finally, accuracy assessments need to be made for different population groups, because the general accuracy rates might be misleading. Apart from issues related to varying performance of facial recognition technology depending on people's sex, age (children and the elderly) and ethnic group, the technology's accuracy when applied to people with disabilities is another important aspect that is rarely considered.

4.2. Data quality and training databases

The accuracy of FRT is strongly influenced by the data quality used to create the software and the quality of data used when deployed. Under the principle of data accuracy – reflected in Article 5 (1) (d) of the GDPR as well as Article 4 (1) (d) of the Law Enforcement Directive – authorities must use information that is accurate and up to date.

Several factors influence the quality of facial images. These include background and object occlusion, illumination and light reflection, ergonomics, age, aging, gender, skin colour and skin conditions.[41] Existing standards for facial images define properties of images showing faces to ensure high quality – for example, the number of pixels between the eyes of a face.[42] While further standards and ways of conducting quality checks are still being discussed and researched, FRT often differentiates between images based on their quality. High quality images, taken under controlled circumstances, are usually referred to as facial images, portraits, or mug shots. Other images are considered of lower quality and have to be considered more cautiously. The quality of images is a serious issue when applying facial recognition technologies to images retrieved from video cameras, as the quality of the image cannot be easily controlled.

Facial recognition software is based on pre-trained models, meaning that the software develops rules for identification of faces based on a database of facial images. This was possible through the increase in the availability of facial images at higher quality and the increase in computing power to process large amounts of data. From a fundamental rights perspective, it is important to know which datasets were used to build the facial recognition software, as this influences the performance of the software. For example, although pre-trained software can be adapted to current use, persistent problems were reported for gender and ethnic groups because the software for facial recognition was often trained mainly on facial images of white men, and much less of women and people belonging to other ethnic groups.[43] Not everyone can access large databases of facial images for developing software due to data protection and property rights. Hence, large IT companies have a distinct advantage when developing their facial recognition software. Yet even among these major vendors of facial recognition software, performance problems persist.[44]

This highlights the importance of having high quality training data for the development of facial recognition technologies and other AI-systems in general, as the use of the systems might lead to discrimination against individuals with certain characteristics, most notably women and girls.[45] In reality, it may be difficult to obtain information about the training data used for developing software. Software might build on already existing algorithms (pre-trained models), which makes it difficult to track back to the original training data. More importantly, vendors of facial recognition software might not want to disclose information about the training data, as was experienced by an expert from a civil society organisation. Copyright issues and trade secrets could be used to block access to information needed to assess the quality of systems employed.[46]

Finally, the quality of images included in the watchlists to be checked against facial images is a crucial discussion in relation to the use of facial recognition technologies. Low quality images on watchlists can considerably increase the number of errors and wrong matches.

41 Sanchez del Rio, J., Conde, C. et al. (2015), *Face-based recognition systems in the ABC e-gates*; FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018.

42 The International Civil Aviation Organization (ICAO) created standards for facial images to be included in travel documents (ICAO 2018, Technical Report. Portrait Quality, Reference Facial Images for MRTD). The International Standard Organization (ISO), together with the International Electrotechnical Commission (IEC), released a standard for Best Practices for Face Images (ISO/IEC 19794-5).

43 Buolamwini, J. and Gebru, T. (2018), 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research* 81:1–15, 2018, Conference on Fairness, Accountability, and Transparency.

44 Grother, P., Ngan, M., and Hanaoka, K. (2018), Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238.

45 FRA (2018), *#BigData: Discrimination and data-supported decision making*, Luxembourg, Publications Office, May 2018; FRA (2019), *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, Luxembourg, Publications Office, June 2019.

46 AI Now Institute (2018), AI Now Report 2018.

5. Use of facial recognition technology by public authorities in the EU

To date, there is no comprehensive overview on the use of facial recognition technology in the EU. Many IT companies offer facial recognition technologies and there is a strong interest in the use of the technology by public administrations for different purposes. This section focuses on their use for law enforcement purposes.[47] A number of tests of facial recognition technologies were carried out during the past years by law enforcement authorities in different EU Member States, although the information available is limited. Apart from test deployments of live facial recognition technologies by public authorities in EU Member States, there is an increased planned use of facial images in the large-scale EU databases in the fields of migration and security (see Section 5.2). Meanwhile, research on the possible use of facial recognition technologies continues (see Section 5.3).

5.1. Testing facial recognition technologies by law enforcement in EU Member States

FRA interviewed representatives of public authorities in Germany, France and the United Kingdom about their possible use and plans of using live facial recognition technologies for law enforcement purposes.

So far, the police in the United Kingdom has been most active in experimenting with live facial recognition technologies. The United Kingdom is the only EU Member State testing live facial recognition technologies in the field with real watchlists. For example, the South Wales Police has used it at major events,[48] and the London Metropolitan Police has carried out several live trials of facial recognition technologies.

The South Wales Police were the first to use live facial recognition technology in the United Kingdom at large sporting events. The police used it at the UEFA Champions League final in June 2017, which brought about 310,000 people to Cardiff. The technology was also used at several further events, including other sports events and music concerts. Several CCTV cameras were placed at different preselected locations. Depending on the size of the events, the police constructed watchlists including several hundreds of people of interest. According to the independent evaluation report from the trials, four different watchlists were used for the UEFA Champions League final. These include:

- a small number of individuals, who were perceived to pose a serious risk to public safety;
- individuals with previous convictions for more serious offense types;
- individuals of possible interest to police, whose presence did not pose any immediate risk or threat to public safety; and
- images of police officers to test the effectiveness of the system.

The watchlists contained between 400 and 1,200 individuals for the different events. The selection was based on different possible criteria. However, no further information on the creation of watchlists was shared with the evaluators of the trial.[49] The absence of information on how watchlists were created makes difficult an assessment of the real purpose, necessity and social need for employing live facial recognition technology. The first case on this issue to come before a court in the European Union (judgment not final) arose in a divisional court in Cardiff. It ruled, in a case directed against the South Wales Police, that the current national legal regime is adequate to ensure the appropriate and non-arbitrary use of the facial recognition technology called "AFR Locate", and that the South Wales Police's use to date of "AFR Locate" has been consistent with

47 To give another example, a Swedish municipality has used facial recognition technology to monitor the attendance of pupils in schools. This has led the Swedish Data Protection Authority to fine the municipality for violating the GDPR. See European Data Protection Board, "Facial recognition school renders Sweden's first GDPR fine", 22 August 2019. In a similar vein, the French data protection authority (CNIL) has also held that the use of facial recognition technology at the entrance of two high schools (in Marseilles and in Nice), for security reasons, appears neither necessary nor proportionate to the given purpose and violates the GDPR. See CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position", 20 October 2019.

48 South Wales Police also tested it for criminal investigation purposes based on CCTV materials, but retrospectively.

49 Davies B., Innes M., and Dawson A., *An evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018. In addition to these deployments to locate people, the South Wales Police used FRT to identify suspects from past crime scenes. Images captured at crime scenes via CCTV or mobile phone cameras are compared against a large database of police custody images for investigation purposes.

day security at public places. Experts stated that facial recognition technologies could make current systems of control more efficient, such as searching for wanted people.

In sum, German and French authorities have tested live facial recognition technologies only on volunteers, without clearly indicating who would be included on watchlists if the technology were to be used for real deployments. Due to the absence of a legal basis for their deployment, live facial recognition technologies could currently not be used legally in these two countries.

Only limited information is currently available on the possible use or tests of live facial recognition technologies in other EU Member States. Austrian authorities bought facial recognition software in 2019 for running facial recognition technologies against databases to identify unknown perpetrators of criminal offences for whom images are available from CCTV cameras or other sources.[56] In the Netherlands, tests have been initiated on the use of facial recognition technologies.

These tests show that a number of Member States are interested in the potential use of facial recognition technologies, whether live (i.e. from CCTV cameras) or not. In some cases, the testing is evaluated either by independent entities contracted by the police, or by the police themselves. Civil society, data protection authorities and academics have raised several fundamental rights concerns with respect to the use of facial recognition technologies.[57] Fundamental rights concerns in relation to the potential use of facial recognition technologies, with a focus on live facial recognition technologies, are discussed in Section 6 and Section 7.

5.2. Facial recognition in large-scale EU IT systems in the area of migration and security

In recent years, the EU developed or upgraded several large-scale IT systems in the field of migration and security. This process is ongoing, with some legislative proposals still pending final adoption.

The Entry/Exit System Regulation introduced facial images as biometric identifiers and provided for the use of facial recognition technology for verification purposes for the first time in EU law.[58] As Table 2 shows, the processing of facial images is meanwhile included in all IT systems, except for the European Travel Information and Authorisation System (ETIAS). The processing of facial images supports biometric verification to check a person's identity, for example, when applying for a visa, crossing the border or requesting asylum. In these cases, the individual concerned is aware that the authorities are taking his or her facial image. This is different from a situation where live facial recognition is applied for identification purposes, without the knowledge of the person affected.

The processing of facial images in large-scale EU IT systems complements the processing of other biometric identifiers, in particular fingerprints. Table 3 provides an overview of the type of biometric data which will be processed in the six EU IT systems once the new legal basis for two of them, Eurodac and the Visa Information System, is in place. Five of the six systems will process facial images.

In the large-scale EU IT systems, the collection and processing of facial images, along with other biometric data, are strictly regulated by law.59 Safeguards limit the collection and further processing of personal data to what is strictly necessary and operationally required. Access to the data is restricted to persons who have an operational need to process the personal data. The legal instruments setting up the IT systems provide for rights of data subjects in line with the EU data protection acquis.[60]

Furthermore, the legal instruments of the upgraded EU IT systems strengthen data quality safeguards. They require that these are met for biometric searches with facial images to be carried out.[61] Typically, they

56 Reply to parliamentary enquiry (*Anfragebeantwortung* 3403/J).

57 See for example in the United Kingdom: Fussey, P. and Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex, Human Rights Centre, July 2019; Big Brother Watch (2019), *Joint statement on police and private company use of facial recognition surveillance in the UK;* and Big Brother Watch*, Face Off Campaign*, May 2019.

58 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, OJ L 327, 9.12.2017, pp. 20-82 (EES Regulation), Arts. 3 (1) (18), 15, and 23-26.

59 See for example Arts. 32-33, read in conjunction with recitals (20), (22) and (54), of Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018, pp. 14-55 (SIS II-borders checks).

60 See e.g. Arts. 51, 52, 53 of the SIS II-border checks Regulation (listing data subjects' rights).

61 See e.g. Art. 33 (4), SIS II-border checks Regulation.

Table 2: EU IT systems for migration and security and processing of facial images

EU IT system		Main provisions on collection and processing of facial images	Purpose	Legal basis
Schengen Information System (SIS II)				
SIS II – police	√	Specific rules for entering biometric data (Art. 42) Specific rules for verification or search with biometric data (Art. 43). [...] Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. [...] (Recital (22))	Enter and process alerts for arrest, missing persons, discreet and specific checks, objects, etc. to safeguard security in the EU and in Schengen Member States	Reg. (EU) 2018/1862, 28 Nov. 2018
SIS II – border checks	√	Specific rules for entering biometric data (Art. 32) Specific rules for verification or search with biometric data (Art. 33) [...] Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. [...] (Recital (20))	Enter and process alerts for the purpose of refusing entry into or stay in the Schengen Member States to support implementation of policies on border checks and immigration	Reg. (EU) 2018/1861, 28 Nov. 2018
SIS II – return	√	'Facial image' to be inserted in alerts on return only to confirm the identity of the person (Art. 4)	Enter and process alerts for third-country nationals subject to a return decision to support implementation of policies on border checks and immigration	Reg. (EU) 2018/1860, 28 Nov. 2018
Entry-Exit System (EES)	√	Facial image of third country nationals (Art. 15) Use of data of data for verification at borders (Art. 23) Use of the EES for examining and deciding on visas (Art. 24) Use of the EES for examining applications for access to national facilitation programmes (Art. 25) Access to data for verification within the territory of the Member States (Art. 26)	Calculating and monitoring the duration of authorised stay of third-country nationals admitted and identify over-stayers Added purpose: law enforcement	Reg. (EU) 2017/2226, 30 Nov. 2017
Visa Information System (VIS)				
VIS	–	Yes (Art. 3 (18))	Facilitate the exchange of data between Schengen Member States on visa applications Added purpose: law enforcement	Reg. (EC) 767/2008, 9 July 2008
VIS proposal	√	Quality of facial images (Art. 9 (8)) Searches based on alphanumerical data and facial images (Art. 18) Specific rules for entering data (Art. 29a)		*Proposal for revision* COM(2018) 302 final, 16 May 2018

European dactylography (Eurodac)				
EURODAC	–	None	Determine the Member State re¬sponsible to examine an applica¬tion for international protection Added purpose: law enforcement	Reg. (EU) 603/2013, 26 June 2013
EURODAC recast proposal	√	Obligation to take fingerprints and facial images (Art. 2) Storage of personal data, including facial images (Arts. 12, 13, 14) Comparison and transmission of all categories of data (Arts. 15, 16)	New purpose: assist with the control of irregular immigration and secondary movements Added purpose: law enforcement	*Proposal for revision* COM(2016) 272 final, 4 May 2016
European Criminal Records Information System (ECRIS-TCN)	√	Facial image only to confirm the identity of a person as result of an alphanumerical and fingerprint data search (Art. 6 (1)) Possibility to use facial images for automated biometric matching in future, provided necessity and proportionality safeguards and readiness of the technology (Art. 6 (2))	Share information on previous convictions of third-country nationals	Reg. (EU) 2019/816, 17 Apr. 2019
Interoperability of EU IT Systems	√	Queries based on alphanumerical and biometric data, including facial images, to be launched with the European Search Portal (ESP) (Art. 9, Interoperability borders and visa; Art. 9 Interoperability police & judicial cooperation, asylum & migration) Biometric templates of facial images to be stored and searched through the biometric matching service (Arts. 13-14, Interoperability borders and visa; Arts. 13-14, Interoperability police & judicial cooperation, asylum & migration) Facial images to be stored in the common identity repository (Art. 18, Interoperability borders and visa; Art. 17, Interoperability police & judicial cooperation, asylum & migration)	Establish a framework for interoperability between EES, VIS, ETIAS, Eurodac, SIS II and ECRIS-TCN to allow for their communication for border management, security, international Added purpose: law enforcement	Reg. (EU) 2019/817 – borders & visa, 20 May 2019 Reg. (EU) 2019/818 – police & judicial cooperation, asylum & migration, 20 May 2019

Notes: = *Facial image. Legislative proposals that have not yet been adopted are presented in italics.*

Source: *FRA, 2019 (based on existing and proposed EU legal instruments)*

Table 3: Biometric identifiers in large-scale EU IT systems for migration and security

				NONE
• Schengen Information System (SIS II) - police	• Schengen Information System (SIS II) - borders • Schengen Information System (SIS II) - return	• Entry-Exit System (EES) • European Criminal Records Information System (ECRIS-TCN) • Interoperability between EU information systems (adopted by EU Parliament on 16/04/19) • European dactylography (Eurodac, recast) • Visa Information System (VIS) (2018 proposal)	• European dactylography (Eurodac) • Visa Information System (VIS)	• European Travel Information and Authorisation System (ETIAS)
 Fingerprints	 Palm prints	 Facial image	 DNA profile	Black = adopted Blue = not adopted

Source: FRA, 2019 (based on adopted and pending legislation)

provide that the automated processing of facial images should be done only as soon as technically feasible to guarantee a reliable match and that the European Commission should report on their readiness. As an additional safeguard, the Agency for the Operational Management of Large-Scale Information Technology Systems (eu-LISA)[62] is responsible for quality assurance safeguards and reports regularly on automated data quality control mechanisms and procedures.[63]

With respect to the Entry/Exit System, the European Commission has adopted technical specifications for the quality, resolution and use of the biometric data, including facial images.[64] With regard to the Schengen Information System, the Joint Research Centre of the European Commission assessed whether face recognition technology is mature enough for its integration into the context of the Schengen Information

62 For an overview of the role and tasks of eu-LISA, see Chapter II of Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, OJ L 295, 21.11.2018, pp. 99-137 (eu-LISA Regulation).

63 See eu-LISA Regulation, Arts. 2 and 12.

64 Annex to the Commission Implementing Decision laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit Systm (EES), C(2019) 1280 final, Brussels, 25 February 2019.

6. Fundamental rights implications of using live facial recognition: general points

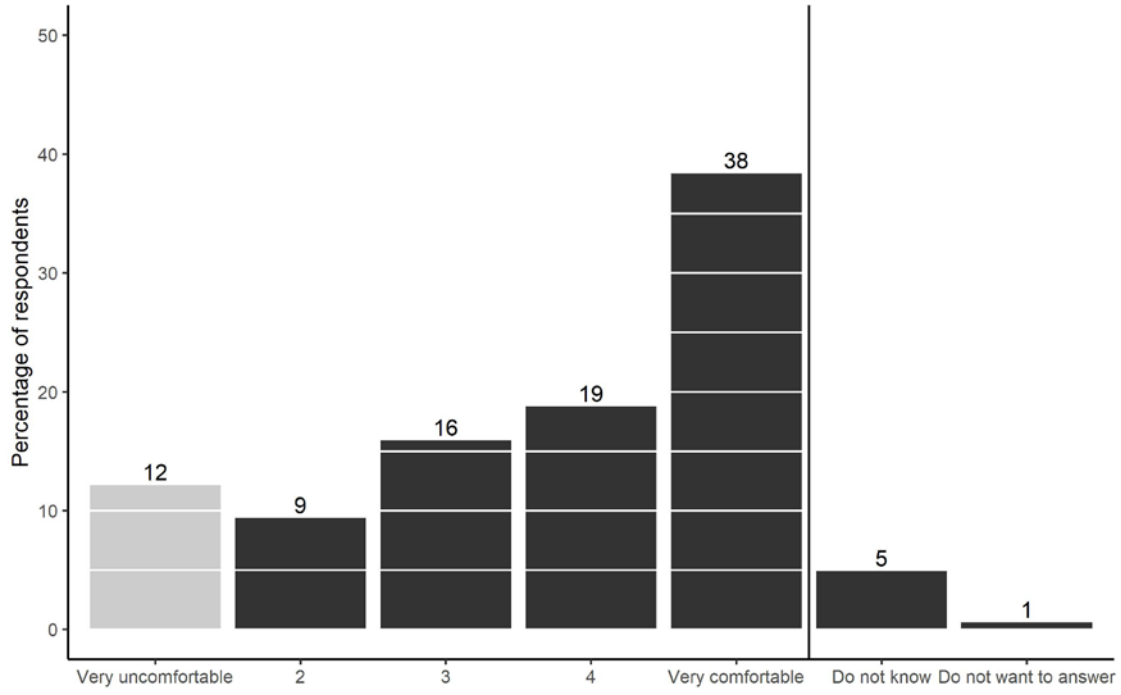
The use of facial recognition technology entails both risks and opportunities for fundamental rights. It entails many fundamental rights challenges that result from the weak position of the individuals whose facial images are captured and then checked against a 'watchlist'. At the same time, facial recognition technology can offer more timely protection – for example by helping to find missing children – and can help to detect fraud and identify theft.

With many unanswered questions linked to the technology's use and accuracy, major concerns with the use of facial recognition technologies and particularly live facial recognition technologies have been voiced by civil society. This section presents how facial recognition is perceived and analyses the fundamental rights implications of such technology in general. Section 7 discusses the individual fundamental rights that are most affected.

6.1. Public perceptions

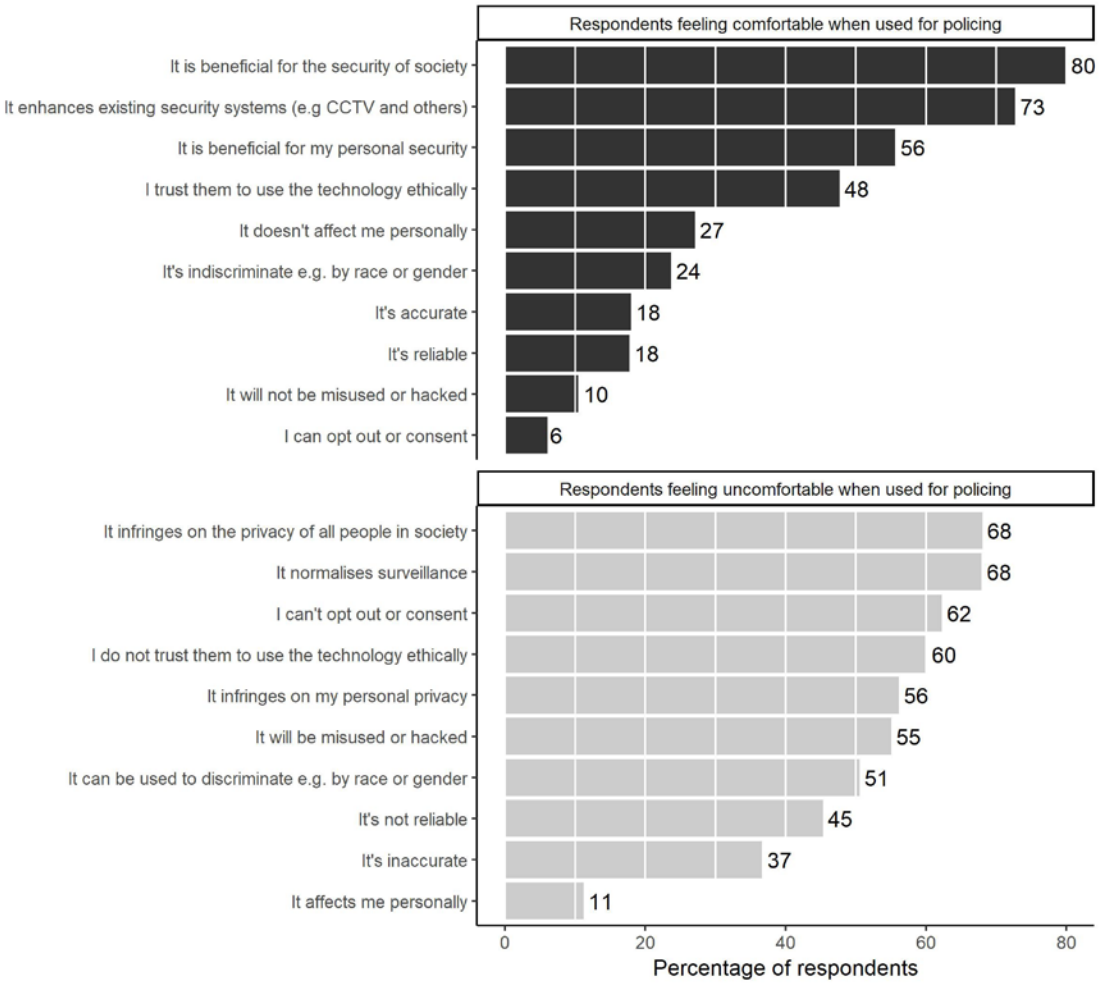
There is no detailed assessment across the EU of the extent to which people find the use of facial recognition technologies intrusive. However, there are indications that a certain share of the population strongly objects to being subjected to facial recognition. In a survey conducted by FRA in 2015 – involving 1,227 third-country nationals at seven border crossing points – 12 % of all respondents indicated feeling very uncomfortable when their facial image was used for crossing the border (see Figure 1); 18 % considered providing a facial image at a border very intrusive to their privacy; and 26 % said that doing so was humiliating. There are differences across nationalities, with Russians and citizens of the United States being less concerned, and Chinese citizens and people from other areas in the world being more concerned. No clear differences with respect to the level of feeling humiliated based on age and gender emerged from the

Figure 1: Travellers' level of feeling comfortable with providing facial images at borders, 2015



Notes: *Question: "How comfortable are you with the use of facial images when crossing the border?"; N = 1,227.*
Source: *FRA, 2015 (based on survey carried out at seven border-crossing points)*

Figure 2: Reasons for people feeling comfortable or uncomfortable when facial recognition is used in the United Kingdom, 2019



Notes: *The upper panel includes respondents who indicated the values 6-10 on the question about feeling comfortable with the use of FRT for policing (on a scale from 1 to 10, where 1 means not comfortable at all, n=2,757). The lower panel includes respondents who indicated not feeling comfortable (values 1-5, n=1,180).*

Source: *Data from Ada Lovelace Institute, 2019, based on an online survey in the United Kingdom*

survey.[73] Results from such a survey might change rapidly over time given the fast development of the technology and that people are more often being exposed to such technology.

According to experts interviewed by FRA, in another survey conducted in the framework of the live facial recognition technologies tested in Nice (France), only three percent of 900 respondents opposed the use of FRT.

A larger survey among the general population about their views on facial recognition was carried out in the United Kingdom.[74] The results of the survey show that, among the general population in the United Kingdom, only 9 % feel completely uncomfortable when facial recognition is used for policing purposes, and 10 % when used at airports. However, 24 % do not feel comfortable with the use of facial recognition in public transport, 28 % at schools, 37 % in supermarkets, and 37 % at the workplace. It appears that, while people generally tend to feel more comfortable with the use of facial recognition technologies for policing purposes, many are not happy with the use of these technologies in everyday life. Figure 2 shows that, according to this survey in the United Kingdom, the

73 Based on FRA (2015), Fundamental Rights Agency Survey results, annexed to eu-LISA, 2015, Smart Borders Pilot Project Technical Report Annexes Volume 2.

74 Ada Lovelace Institute (2019), Beyond face value: public attitudes to facial recognition technology.

main reasons for feeling comfortable are linked to increased security, whereas the main reasons for feeling uncomfortable are related to interferences with people's privacy.

6.2. Requirements for justified interference with fundamental rights

Full compliance with fundamental rights is a prerequisite for any law enforcement activities, irrespective of the technologies used. EU and international human rights law provide a normative framework for the design, development and deployment of facial recognition technologies. They help determine whether or not a specific use of facial recognition technology is human rights compliant.[75]

Section 7 examines the main fundamental rights affected by facial recognition technologies. These are typically not absolute rights, so can be subject to limitations.[76] This sub-section presents the steps that need to be followed to determine whether or not a Charter right can be limited. Requirements that are specific to an individual right (in particular those relating to interferences with the right to respect for private life and protection of personal data) are analysed in Section 7.

So far, the tests and deployments of facial recognition technologies in EU Member States by public authorities mainly focused on technical accuracy and did not assess fundamental rights implications more broadly. A strong focus was put on image quality and error rates. These results are important – but are only one aspect. If facial recognition technology were perfect in terms of accuracy, other questions would nonetheless remain. For example, live facial recognition technology, which involves subjecting people to facial recognition potentially without their informed consent, puts them in a weak and potentially humiliating position.

The use of live facial recognition technologies thus also relates more broadly to the right to human dignity. Human dignity is the foundation of all fundamental rights guaranteed by the EU Charter of Fundamental Rights.[77] Article 1 of the Charter states that human dignity is inviolable and that it must be respected and protected. The Court of Justice of the EU (CJEU) has confirmed in its case law that the fundamental right to dignity is part of EU law.[78]

Biometric data, including facial images, must be processed in a manner that respects human dignity. The processing of facial images may affect human dignity in different ways, as the following examples illustrate:

- People may feel uncomfortable going to public places under surveillance. They may change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events. Depending on the extent to which live facial recognition technologies are applied, the impact on what people may perceive as surveillance technologies on their lives may be so significant as to affect their capacity to live a dignified life.

- FRA documented examples where authorities used excessive force to take the fingerprints of people who arrived at the border.[79] Similar situations may hypothetically also occur to force people to go through places where facial images are captured. The prohibition of excessive use of force deriving from Article 4 of the Charter, which prohibits torture, inhuman and degrading treatment, is a key safeguard when taking any biometric data from individuals.[80]

- When law enforcement authorities obtain many hits when deploying facial recognition technologies (for example during a large public event), they may need to stop and check a larger number of people. This poses high demands on police staff, particularly when many people are wrongly stopped due to an erroneous match, as may likely be the case when the facial image is extracted from CCTV cameras. The risk of inappropriate police behaviour due to stress increases, potentially undermining the dignity of the person stopped. Interacting with people who have been subject to a match requires particular attention. Officers

75 See also, Fussey, P. and Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex, Human Rights Centre, July 2019, p. 31; McGregor, L., Murray, D. and Ng, V. (2019), 'International Human Rights Law as a Framework for Algorithmic Accountability', International and Comparative Law Quarterly 68 (2019), pp. 309-343.

76 Scheinin, M. and Sorell, T. (2015), *SURVEILLE Deliverable D4.10 – Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, p. 8.

77 Barak, A. (2019), 'Human dignity as a framework right (mother-right)', in Barak, A., *Human Dignity: The Constitutional Value and the Constitutional Right*, Cambridge, Cambridge University Press, 2015, Chapter 9 (pp. 156-169).

78 CJEU, C-377/98, *Netherlands v. European Parliament and Council*, 9 October 2001, paras. 70-77.

79 FRA (2018) *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 52-55; FRA (2019), *Fundamental Rights Report 2019*, Luxembourg, Publications Office, June 2019, p. 133.

80 FRA (2018) *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018.

need adequate training on the need to ensure full respect of the right to human dignity and on how to avoid the risk of tensions, including when dealing with vulnerable people. Civil society representatives in the United Kingdom initiated legal action against the South Wales Police for fining a person who tried to cover their face when live facial recognition technology was being tested.

An important way to promote compliance with fundamental rights is oversight by independent bodies. This applies to many different areas, ranging from the oversight of child protection authorities in case of children at risk of exploitation, abuse or neglect to international monitoring bodies established to prevent torture, inhuman or degrading treatment. Independent supervision is also an essential component of European data protection law,[81] with Article 8 (3) of the Charter making express reference to it. In light of the fundamental rights issues at stake and its complexity, independent supervision is essential to genuinely protect people whose rights may be affected by facial recognition technology.

Turning to fundamental rights that may be subject to restriction, Article 52 (1) of the Charter sets the framework. Interferences with fundamental rights can only be justified if they respect the requirements of the Charter and of the ECHR, in case of Charter rights corresponding to rights guaranteed in the ECHR (Article 52 (3) of the Charter).[82]

Pursuant to Article 52 (1) of the Charter, any limitation on fundamental rights must:

- be provided for by law,
- genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others,
- respect the essence of the right,
- and be proportionate.[83]

The CJEU has underlined that all of these requirements must be complied with. The court has also emphasised that any limitation on the exercise of the rights and freedoms recognised by in the Charter must respect "the essence" of those rights and freedoms.[84] This means that fundamental rights can be limited to a certain extent, but not completely disregarded. Once it has been established that the inalienable, essential core of a right is not violated by a measure, the necessity and proportionality test as outlined in the Charter is to be conducted as a next step in respect of non-core aspects of that right.[85]

An objective of general interest – such as crime prevention or public security – is not, in itself, sufficient to justify an interference. Any interference with a Charter right needs to be examined as to whether the given legitimate aim could not be obtained by other means that interfere less with the right guaranteed. [86]

Similar requirements are also imposed by the ECHR, as interpreted by the European Court of Human Rights (ECtHR). A three-pronged test developed by the ECtHR requires that any rights interference has to pursue a legitimate aim; be in accordance with the law, i.e. necessitating an appropriate legal basis meeting qualitative requirements (public, precise, and foreseeable);[87] as well as necessary in a democratic society (necessity and proportionality test).[88] As a fourth test, the ECtHR also used the 'essence of a right' concept, which can be derived from the object and purpose of the ECHR as a whole.[89] The case law of the ECtHR has identified the following elements when determining whether a measure is "necessary in a democratic society" – for example, that the interference needs to correspond to a pressing social need, must be proportionate, and that the reasons given to justify the interference

81 Law Enforcement Directive, Chapter VI; GDPR, Chapter VI.

82 Charter, Art. 52 (3): "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention."

83 As also reiterated and explained by the CJEU, see for example C-73/07, *Satakunnan Markkinapörssi and Satamedia*, 16 December 2008, para. 56; Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke* and *Eifert GbR and Hartmut Eifert*, 9 November 2010, para. 77; Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 52; C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 92; and C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 December 2015, paras. 69 and 80-82.

84 See CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, paras. 94-95, which refer to Article 52 (3) of the Charter. See also Scheinin, M. and Sorell, T. (2015), *SURVEILLE Deliverable D4.10 – Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, 7 April 2015, p. 9.

85 See e.g. Brkan, M. (2019), 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning', *German Law Journal* 20 (2019), p. 867.

86 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014.

87 On the requirements of "quality of law", see ECtHR, *Gorlov and Others v. Russia*, Nos. 27057/06, 56443/09 and 25147/14, 2 July 2019, para. 97.

88 See e.g. ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, paras. 95-104.

89 Scheinin, M. and Sorell, T. (2015), *SURVEILLE Deliverable D4.10 – Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, 7 April 2015, p. 9.

must be relevant and sufficient.[90] In respect to the use of new technologies, the ECtHR observed in *S. and Marper v. the UK* that States should "strike a right balance" between protecting fundamental rights and developing new technologies.[91] This also applies when introducing facial recognition technologies to help support law enforcement and border management.

This assessment needs to be carried out for each way of using the technology. It must cover all relevant fundamental rights and take into account all elements, ranging from the legitimate purpose the technology wants to achieve and the way the facial images are captured (e.g. CCTV cameras, body-worn cameras, mobile phone applications, etc.) to the degree of errors it entails, so as to enable an informed assessment of the necessity and proportionality of its use. The more intrusive the technology is, the stricter the test must be.

As regards its legitimate objective, the results of the necessity and proportionality test will be different depending on whether it supports the verification of the identity of a person – as, for example, during border checks at airports (one-to-one comparison); or whether it is used in criminal investigations to run the facial image of a person against a watchlist (one-to-many comparison). In this second case, the seriousness of the crime being investigated plays an important role. The examples of its use listed in Section 5 indicate that, in general terms, the authorities deployed or tested the technology to enhance efficiency in police work in terms of increased success in finding wanted people and reducing costs. Authorities also mentioned the inability of human work force to go through all video footage produced by CCTV cameras as a justification for testing facial recognition technologies. FRA was not able to obtain a comprehensive picture of the types of crimes for which law enforcement authorities used or tested the technology.

Concerning accuracy, the results from the tests in Nice were reported to have worked perfectly, without any errors. However, the use of facial recognition technologies usually comes with errors. The largest accuracy test of facial recognition technologies is available from the US Department of Commerce's National Institute of Standards and Technology (NIST), conducting an ongoing vendor test on verification and identification. The results show a strong increase in accuracy rates, currently below 0.2 % for galleries of 12 million individuals.[92] Yet there is a complex relationship between false positives (i.e. stopping innocent people) and false negatives (i.e. not being able to find the person of interest). A proportionality assessment needs to balance the trade-off between the two as illustrated below. The question is what number of innocent people being flagged by the system and stopped by the police is acceptable for the sake of possibly succeeding in finding a person of interest. The outcome of this assessment varies depending on the importance of finding a specific person and the harm done by stopping innocent people.

A vivid example comes from the test carried out in Germany. When using three different facial recognition software systems in parallel, analysing matches in cases when at least one of the three systems provided a match, the tests in Berlin had an average miss rate (false negatives among all negative) of 8.8 %, with a false positive identification rate of 0.34 %. This means that in just under one in ten cases – on average and in the long run – a person of interest would be missed (or in just over nine in ten cases identified). At the same time, out of every 1,000 people crossing the system, between three and four people would be wrongly identified as matches by the system. According to the German authorities, this is not acceptable, because considering the number of people crossing train stations every day, this would lead to a large number of people incorrectly stopped (or at least flagged to the police). The system can also be used to provide a match only when all three software systems agree. This would increase the miss rate to 31.9% (meaning in one in three cases – in the long run – a person of interest would be missed), and reduce the false positive identification rate to 0.00018 %. This is considered very low by the authorities conducting the test.[93] Used at a station with 100,000 people crossing every day, such a rate would mean that, over a period of ten days, about two people would be flagged despite not being in the system.[94]

90 See, for instance ECtHR, *Khelili v. Switzerland*, No. 16188/07, 18 October 2011; ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008; ECtHR, *K & T v. Finland*, No. 25702/94, 12 July 2001; ECtHR, *Z v. Finland*, No. 22009/93, 25 February 1997; ECtHR, *Huvig v. France*, No. 11105/84, 24 April 1990; ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

91 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, para. 112.

92 Grother, P., Ngan, M., and Hanaoka, K. (2018), Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238.

93 *Polizeipräsidium Potsdam*, Biometrische Gesichtserkennung, 2018.

94 It is important to mention that results from tests are subject to uncertainty due to statistical variation and not true values.

7. Fundamental rights most affected

This section discusses the specific fundamental rights that are most affected when using facial recognition technologies in the context of law enforcement. It focuses on live facial recognition technologies, when facial images are extracted from CCTV cameras and compared with a database or watchlist. This section is not an exhaustive analysis of all fundamental rights affected by facial recognition technologies, but rather of pertinent examples.

7.1. Respect for private life and protection of personal data

The rights to respect for private life and data protection are central to the deployment of facial recognition technology in public places. Although the two are closely related, they are distinct, self-standing rights. They have also been described as the "classic" right to the protection of privacy and a more "modern" right, the right to data protection.[95] Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They thus form an essential prerequisite for the exercise of other fundamental rights, such as the freedom of thought, conscience and religion (Article 10 of the Charter), freedom of expression and information (Article 11 of the Charter), and freedom of assembly and of association (Article 12 of the Charter).[96]

Using live facial recognition technologies implies collecting, comparing and/or storing facial images in an IT system for identification purposes. It, therefore, constitutes an interference with the right to protection of personal data set out in Article 8 of the Charter (embodying pre-existing EU data protection law) and the right to private life under Article 7 of the Charter and Article 8 of the ECHR. Facial images constitute personal data, as also confirmed by the CJEU[97] and the ECtHR.[98] The ECtHR has also stated that a person's facial image constitutes one of the key attributes of his/her personality, as it reveals the person's unique characteristics and distinguishes the person from his/her peers. The right to the protection of one's facial image is thus one of the essential components of personal development.[99]

The concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person, and can, therefore, embrace multiple aspects of the person's physical and social identity.[100] There is also a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[101] In other contexts, the ECtHR has used the concept of "reasonable expectation of privacy" – referring to the extent to which people can expect privacy in public spaces without being subjected to surveillance – as one of the factors, albeit not necessarily a conclusive one, to decide on a violation of the right to respect for private life. Its relevance and scope of application, however, appears to be limited.[102] Similarly, according to UN experts, the mere fact that participants in assemblies are out in public does not mean that their privacy cannot be infringed.[103] The processing of facial images in large-scale databases may, as facial recognition technology develops, raise unchartered issues about the rights to protection of private life as well as of personal data. Given that these two rights are not absolute rights, they can be subject to limitations, but any interference needs to be adequately justified[104] and cannot compromise at any event the essential, inalienable core of that right, as explained in Section 6.2.[105]

Live facial recognition technology involves the biometric processing of facial images taken in a public place, for the purpose of determining a person's

95 CJEU, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert, Opinion of Advocate General Sharpston*, 17 June 2010, para. 71.

96 FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition*, Luxembourg, Publications Office, June 2018, p. 19.

97 CJEU, C-291/12, *M. Schwarz v. Stadt Bochum*, 17 October 2013, paras. 22, 48-49.

98 ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016, para. 56.

99 ECtHR, *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, Strasbourg, Council of Europe, 31 August 2019, para. 138.

100 ECtHR, *López Ribalda and Others v. Spain*, Nos. 1874/13 and 8567/13, 17 October 2019, para. 87.

101 *Ibid.*, para. 88.

102 Vermeulen, M. (2015), *SURVEILLE Deliverable D4.7 – The scope of the right to private life in public places*, July 2014, p. 2.

103 UN, Human Rights Committee, *draft General Comment No. 37 [Article 21: right of peaceful assembly)*, draft prepared by the Rapporteur, Christof Heyns, July 2019, para. 69.

104 See also FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition*, Luxembourg, Publications Office, June 2018, pp. 35-52.

105 European Court of Human Rights (2019), *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*, Strasbourg, Council of Europe, updated on 31 August 2019, paras. 133 and 136.

identity (one-to-many identification) and the potential retention of those images. Consequently, both the initial biometric processing of facial images, any subsequent retention of video footage, and comparing the data to a 'watchlist' – alongside populating the watchlist with facial images – constitute interferences with the right to respect for private life and the protection of personal data.[106] Given that processing of personal data constitutes a limitation of these rights, it needs to be subjected to a strict necessity and proportionality test, including a clear legal basis to do so and a legitimate aim pursued. Such a test has to take into account the context and all circumstances at hand. Hence, the sensitivity of the data or the way the data are used are important for the context.[107]

Next to the fundamental rights safeguards and key data protection principles flowing from Article 8 of Charter as interpreted by the CJEU, specific guarantees under the EU data protection acquis further corroborate the necessity and proportionality test outlined in Section 6.2. Pursuant to Article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Article 10 of the Law Enforcement Directive lays down similar, albeit a bit more permissive conditions.[108]

Collecting and processing facial images for the purpose of FRT needs to be strictly in line with European data protection law. Following the main legal principles of data protection, processing facial images must be

a) lawful, fair and transparent;

b) follow a specific, explicit and legitimate purpose (clearly defined in Member State or Union law); and

c) comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability.[109]

Lawful, fair and transparent

Transparent and clear provision of information is of utmost importance in the context of live facial recognition technologies, since people's facial images are usually captured by cameras at public places without their knowledge and consent. The GDPR and the Law Enforcement Directive include provisions guaranteeing the principle of transparency and the right to information. The right to personal data protection requires fair processing, which includes adequately informing persons whose facial images are taken. Article 5 (1) of the GDPR stipulates that "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". Recital (26) of the Law Enforcement Directive echoes the same requirements. Also, the right to information is a precondition for the child to exercise their right to be heard in judicial and administrative proceedings that affect them, which is protected by Article 12 of the CRC and Article 24 (1) of the Charter. Provision of information is not only a transparency requirement under European data protection law, but it also promotes respect for dignity of the individual.

Controllers must take appropriate measures to provide information related "to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[110] Articles 13 and 14 of the GDPR and the Article 13 of the Law Enforcement Directive require that individuals be informed on the identity and the contact details of the controller, the purpose of the processing of data, retention times, the right to request access to stored data, and its erasure or rectification, as well as the right to lodge a complaint with a supervisory authority. However, the Law Enforcement Directive carves out some possible exceptions under this obligation in Article 13 (3), to avoid obstructing or prejudicing ongoing investigations; or to protect public security and national security. These scenarios are of major importance when facial recognition technologies are considered. The potential purposes currently discussed and invoked for the use of facial recognition technologies might only work without informed consent or without the possibility to opt out (e.g. in case of searching terrorists or other suspected criminals). Hence, this limitation on the fundamental right to be informed and consent to the processing of data, paired with the restrictions on the right to access to stored data, needs to be strongly justified.

106 Fussey, P. and Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex, Human Rights Centre, July 2019, p. 36.

107 EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.

108 For a more elaborated and detailed presentation of the necessity and proportionality test under European law, consult FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, pp. 35-38.

109 Law Enforcement Directive, Art. 4; GDPR, Art. 5.

110 Law Enforcement Directive, Art. 12; GDPR, Art. 12 (1).

The European Data Protection Board (EDPB) clarifies that Member States have the obligation to inform individuals of existing video surveillance devices. Such information should be provided through a warning sign at a reasonable distance of the monitored places, and information that is accessible without entering the area under surveillance. This may include an information sheet, a link to a website detailing information on the surveillance, a telephone number to receive further information, or an app mapping the location of video devices.[111]

The process of extracting biometric features from a face, which makes the face available for processing in other ways, changes the level of intrusion due to the availability of new technological means. As a consequence, the availability of a facial image in a database is different from applying a software that extracts unique features from a facial image, irrespective of whether the extracted features are in fact run against a watchlist. Following the argumentation of the Data Protection Commissioner of the City of Hamburg, a previously legally specified balance between authorities' interference for the purpose of law enforcement and the right to informational self-determination, is changed massively to the detriment of the latter. Moreover, the Data Protection Commissioner sees facial recognition technologies as providing for an entirely new way of intrusion and opportunities of persecution, which requires a stand-alone, specific regulation.[112]

Specific, explicit and legitimate purpose

The principle of purpose limitation is one of the fundamental principles of European data protection law.[113] It is mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the GDPR and Article 4 (1) (b) of the Law Enforcement Directive. It requires that personal data are processed only for specified purposes, which must be explicitly defined by law. The person concerned should be able to foresee the purpose for which their data will be processed.[114] These principles equally apply in the context of processing data via facial recognition technologies. The principle of purpose limitation also implies the prohibition of the unlimited retention of such data.

In this context, the purpose of processing facial images via facial recognition technologies must be strictly determined – with a high threshold, essentially consisting of the purpose to combat terrorism and other forms of serious crime, which is the well-established purpose limitation under EU law for law enforcement access to various large-scale EU databases. As an additional purpose, it could also be used to identify missing persons and victims of crime, including children.

By designing IT systems, including facial recognition systems, for combating serious crimes and terrorism, improving public safety, and curbing irregular migration, there is a risk of function creep – meaning that the personal data (the facial images) may be used for purposes that were not initially envisaged. In the case of interoperability of large-scale EU databases, safeguards need to be implemented to ensure that facial image recognition technology is not unlawfully used to access EU large-scale databases.[115]

Data minimisation, data accuracy, storage limitation, data security and accountability

Data must be also safely collected, processed and stored and unlawful data processing must be prevented and detected.[116] A related issue is the prevention of unauthorised access to and use of the personal data processed by facial recognition technologies. Article 32 of the GDPR and Article 29 of the Law Enforcement Directive both require Member States to take necessary measures to avoid that personal data are disclosed to, or accessed by, unauthorised persons or organs. If facial recognition systems are made interoperable with other IT systems in future, ensuring purpose limitation in such a scenario will be particularly challenging. To avoid potential data leakages, ongoing research looks into ways to protect the privacy of biometric data and hence increasing data security. Current research assesses

111 European Data Protection Board (2019), *Guidelines 3/2019 on processing of personal data through video devices – version for public consultation*, Brussels, 10 July 2019, pp. 21-23.

112 *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (2018).

113 FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition*, Luxembourg, Publications Office, June 2018, p. 122; Article 29 Data Protection Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 2013, 00569/13/EN, Brussels, 2 April 2013.

114 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Opinion of Advocate General Kokott, 18 July 2007, para. 53.

115 For more on the fundamental rights implications of interoperability of large-scale IT systems, see FRA (2018), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion 1/2018 [Interoperability], Vienna, 11 April 2018.

116 For a comprehensive overview of the European legal framework on data protection, see: FRA, Council of Europe and EDPS (2018), *Handbook on European data protection law. 2018 edition*, Luxembourg, Publications Office, June 2018.

Automated decision making and the right to human review

Article 22 of the GDPR and Article 11 of the Law Enforcement Directive generally forbid automated decision making, meaning any "decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." The exception to this prohibition is when this is authorised by Union or Member State law, which provides for appropriate safeguards for the rights and freedoms of the data subject, at least the right to human intervention on part of the controller. When special data are involved, such as facial images, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place.

All trials and deployments envisaged in EU Member States do provide for human intervention. This means that matches based on facial recognition technologies are flagged to humans (e.g. police officers), who will evaluate the match and based on this evaluation take action. Many false positives are already ruled out at this stage.

However, the concept of 'automated' decision making is elusive and needs further discussion and research. For example, in some cases human intervention might be to simply 'sign-off' on all outcomes of the system, hence rendering it virtually automated.* Contrary to that and as another example, if humans review and potentially override outcomes of the system, this needs to be evaluated as well. Research indicates that humans overrule outcomes from algorithms mainly when the result is in line with their stereotypes (for example, again putting minority groups at a disadvantage). This behaviour threatens the possible added value of the automated processing through potentially being more accurate or in cases even fairer than humans.**

* *Veale, M. and Edwards, L. (2018), 'Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling', Computer Law & Security Review, Vol 34 (2), April 2018, pp. 398-404.*

** *Green, B. And Chen, Y. (2019), 'Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments', In FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019.*

technological solutions to protect biometric identifiers (templates).[117]

EU law requires data controllers to protect data by design, meaning that measures need to be put in place to integrate safeguards to protect the rights of people concerned.[118] As a consequence, when planning to use facial recognition technologies, a fully-fledged analysis, plan and process for protecting rights needs to be made from the outset. Pursuant to the GDPR and the Law Enforcement Directive, the use of facial images requires a Data Protection Impact Assessment (DPIA), including prior consultation with the data protection authority (DPA).[119] Data Protection Impact Assessments are important tools to comprehensively assess the legal permissibility of and risks involved in using facial recognition technologies and they need to be thoroughly done. The role of the DPAs is crucial in this respect for safeguarding fundamental rights, as independently acting bodies established by law.[120]

Indeed, tests on facial recognition technologies made some efforts to conduct an impact assessment. The German test included a data protection plan set up with the DPA for the purpose of the test. The draft impact assessment of the South Wales Police was also published,[121] as was the assessment of the London Metropolitan Police.[122] The police in France informed the DPA a few weeks before the trial about their plans of carrying out the test.

117 Gomez-Barrero M., et al. (2018): 'General Framework to Evlauate Unlinkability in Biometric Template Protection Systems', *IEEE Transactions on Information Forensics and Security*, vol. 13(6), pp. 1406-1420.

118 Law Enforcement Directive, Art. 20 (1); GDPR, Art. 25 (1).

119 Law Enforcement Directive, Arts. 27-28; GDPR, Arts. 35-36.

120 Further information on how to conduct Data Protection Impact Assessments, including in the context of video surveillance, are included in the Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, as last revised and adopted on 4 October 2017.

121 Draft South Wales Police Privacy Impact Assessment, Version 4.0, 2018.

122 London Police Ethics Panel, Interim Report on Live Facial Recognition, 2018.

7.2. Non-discrimination

Discrimination is "where one person is treated less favourably than another is, has been or would be, treated in a comparable situation" on the basis of a perceived or real personal characteristic[123] (called 'protected grounds/characteristics'). Article 21 of the Charter prohibits any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The Charter prohibition reflects corresponding rights in the ECHR (Article 14) and in Protocol No. 12 to the ECHR (Article 12), but is even broader. This formulation established a non-exhaustive, open list extending protection to a wide range of new grounds; and unlike Article 14 of the ECHR, the Charter right to non-discrimination is a freestanding right applying to situations that do not need to be covered by any other Charter provision.[124] Article 20 of the EU Charter provides that everyone is equal before the law.

Justification for different or less favourable treatment is possible under the ECHR and EU law. Differential treatment may be justified where it pursues a legitimate aim and where the means to pursue that aim are necessary and proportionate.[125] These boundaries may vary on a case-by-case basis, depending on the circumstances of the individual case. For instance, in ECtHR jurisprudence, differential treatment relating to matters to be at the core of personal dignity (e.g. race or ethnic origin, gender, private life) are more difficult to justify than in other areas. [126]

Discrimination in data-supported algorithmic decision making can occur due to several reasons. Discrimination can occur during the design, testing and implementation of algorithms used for facial recognition, through biases that are incorporated – consciously or not – in the algorithm itself, as well as when officers decide what action to take following a match. If there are differences in the performance of an algorithm, it is usually very difficult and sometimes impossible to remove the bias through mathematical or programmatic solutions.[127] An important cause of discrimination is the quality of data used to develop algorithms and software.[128] To be effective and accurate, facial recognition software needs to be fed with large amounts of facial images. More facial images lead, in principle, to more accurate predictions. However, accuracy is not only determined by the amount of facial images processed but also by the quality of such facial images. Data quality requires also a representative set of faces reflecting different groups of people.[129] Yet to date, facial images used to develop algorithms in the Western world often over-represent white men, with lower numbers of women and/or individuals of other ethnic backgrounds. As a result, facial recognition systems worked well for white men, but not for black women.[130]

Phenotypical characteristics – i.e. the expression of genes in an observable way, such as hair or skin colour – might influence the outcome of biometric matching in facial recognition systems: reflection of light affects the quality of facial images of very fair-skinned persons, and not enough light affects the quality for very dark-skinned persons.[131] When comparing their facial images against a database or watchlist, such people are, therefore, exposed to a higher likelihood of being wrongly matched as false positives. This may result in certain groups of persons being wrongly stopped more frequently due to their colour of the skin.

Article 26 of the Charter guarantees the rights of persons with disabilities. Disability must not result in unequal treatment or discrimination prohibited

123 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, pp. 22-26, Art. 2; and Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, 2.12.2000, pp. 16-22, Art. 2.

124 FRA and CoE (2018), *Handbook on European non-discrimination law. 2018 edition*, Luxembourg, Publications Office, June 2018, p. 35.

125 See for example ECtHR, *Burden v. the United Kingdom [GC]*, No. 13378/05, 29 April 2008, para. 60; ECtHR, *Guberina v. Croatia*, No. 23682/13, 22 March 2016, para. 69. For the justification test in EU law, see CJEU, C-356/12, *Wolfgang Glatzel v. Freistaat Bayern*, 22 May 2014; CJEU, Case 170/84, *Bilka-Kaufhaus GmbH v. Karin Weber Von Hartz*, 13 May 1986.

126 FRA and CoE (2018), *Handbook on European non-discrimination law. 2018 edition*, Luxembourg, Publications Office, June 2018, p. 93.

127 FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, p. 26; FRA (2018), *#BigData. Discrimination in data-supported decision making*, Luxembourg, Publications Office, May 2018. However, there is ongoing research looking into this aspect particularly from privacy and non-discrimination point of view. See for example the SensitiveNets website, and A. Morales, A., J. Fierrez, J., and R. Vera-Rodriguez, R. (2019), SensitiveNets: Learning Agnostic Representations with Application to Face Recognition. arXiv:1902.00334, 2019.

128 FRA (2019), *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, Luxembourg, Publications Office, June 2019.

129 *Ibid.*

130 Center on Privacy and Technology at Georgetown Law (2016), The Perpetual Line-Up; and Buolamwini, J., and Gebru, T. (2018), 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Proceedings of Machine Learning Research 81:1–15, 2018, Conference on Fairness, Accountability, and Transparency.

131 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 17.

by Articles 20 (equality before the law) and 21 (non-discrimination) of the Charter. There is a lack of research and little discussion on how facial recognition technologies (and artificial intelligence more broadly) affect people with disabilities. The types of disabilities are manifold. Not much information is available on the extent to which facial recognition technologies work accurately for different forms of disabilities or injuries to the face, such as people whose face has been altered as a result of an accident or paralysis, people who had facial surgeries or people with craniofacial differences.[132] More research is needed to understand whether facial recognition technologies may discriminate against people with certain disabilities.

Although the awareness of the risk of discrimination by facial recognition technologies has increased considerably over the past years, many professionals still do not see this is an issue. Some public officials FRA interviewed indicated that discrimination is not a problem because the 'technology is neutral' or were confident that the system works equally for different groups because people from different groups were included when testing it. In fact, none of tests described in this paper analysed the results in terms of different performance by ethnic origin, sex or age. Some of the tests did not even have enough dark-skinned people among volunteers to test differences in the performance. Therefore, a much larger sample of people would have been needed to test for possible discrimination. The largest test of facial recognition technologies in the United States shows that error rates differ according to demographic characteristics, including age, sex and country of origin. Moreover, the results in terms of differences by characteristics also differ across software systems.[133]

Discrimination in facial recognition technologies might have an adverse effect on group cohesion, if people from specific ethnic groups are disproportionally more often erroneously stopped. This can significantly affect their trust in the police or border management officials.[134]

7.3. Rights of the child and of elderly people

Facial recognition systems affect the rights of children in different ways. Article 24 of the Charter (rights of the child) emphasises that the best interests of the child must be a primary consideration in all actions public authorities and private actors take concerning children. EU Member States must provide the child with such protection and care as is necessary for the child's well-being and development. The best interests of the child is one of the four core principles of the UN Convention on the Rights of the Child (CRC).[135] The child's best interests must also be given a primary consideration in the context of using facial recognition technology for law enforcement and border management purposes. The CJEU has also expressly recognised the need to respect children's rights and requires Member States to take due account of the CRC when implementing EU law.[136] The EU data protection acquis provides special protection to children with regard to their personal data.[137]

Due to the particular vulnerability of children, the processing of their biometric data, including facial images, must be subject to a stricter necessity and proportionality test, compared to adults.

In addition, as the child grows and time passes, the accuracy of a biometric match diminishes. The risk of a wrong match increases when facial images recorded at a young age are compared more than five years after they were collected.[138] Present technologies for facial recognition guarantee a reliable match when the child was at least six years old when the biometric facial image was captured and the match happened within a time frame of five years. In general, research indicates that the accuracy of facial recognition technology is significantly lower for children younger than 13 years.[139] Software tests clearly indicate that images of younger people

132 See Medium, "Disability and AI-Bias", 11 July 2019.

133 Grother, P., Ngan, M., and Hanaoka, K. (2019), Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification, 2019/04/12.

134 FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, p. 39.

135 United Nations Convention on the Rights of the Child, New York, 20 November 1989 (1577 U.N.T.S., p. 3).

136 CJEU, C-540/03, *European Parliament v. Council of the European Union* [GC], 27 June 2006, paras. 37, 57; CJEU, C-244/06, *Dynamic Medien Vertriebs GmbH v. Avides Media AG*, 14 February 2008, para. 39. For a comprehensive overview on the protection of children's rights under EU law, see FRA and CoE (2015), *Handbook on European Law relating to the rights of the child*, Luxembourg, Publications Office, November 2015.

137 See GDPR, recitals (38) and (58).

138 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 109.

139 Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen (2013), *Fingerprint Recognition for Children*, Luxemburg, Publications Office, September 2013; Chaudhary, A., Sahni, S., and Saxena, S. (2014), 'Survey: Techniques for Aging Problems in face recognition', *MIT International Journal of Computer Science and Information Technology*, Vol. 4 (2), August 2014, pp. 82-88; Ramanathan, N., Chellappa, R., and Biswas, S. (2009), 'Computational methods for modelling facial aging: A survey', *Journal of Visual Languages and Computing* 20, pp. 131–144; Galbally, J., Ferrara, P., Haraksim, R., Psyllos, Al, and Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Luxembourg, Publications Office, July 2019, pp. 16, 112.

result in considerably more false negatives (misses) compared to other age groups, most probably due to rapid growth and change in facial appearance.

Ageing, i.e. the time between an image is taken and when it is compared, negatively affects the accuracy of facial recognition technologies.[140] Scientific research does not allow for conclusions on the reliability of a match when more than five years have passed. The same holds true for facial images of older people if compared to images taken many years earlier.

When addressing the issue of blanket retention of biometric data for law enforcement purposes of persons not convicted of a crime, the ECtHR emphasised in S. and Marper v. the UK that this may be especially harmful in case of children, given their special situation and the importance of their development and integration into society.[141] Moreover, when facial recognition is used to prevent, detect and investigate terrorism and other serious crime, it is difficult to see how this may justify the processing of facial images of children below the age of criminal responsibility.[142]

At the same time, in some cases, the impact of facial recognition technology on the best interests of the child may also be positive. Facial recognition systems can contribute to protecting the right of the child to preserve their identity.[143] In line with the CRC, where a child is deprived of some or all of the elements of their identity, States must provide appropriate assistance and protection, with a view to quickly re-establishing the identity of the child.[144] Facial recognition systems used by the police and border guards may help trace missing and abducted children, including child victims of crime, and prevent child abduction. FRA's small-scale survey at border posts shows that children reported as missing are frequently encountered at border-crossing points.[145]

As a result, facial recognition technologies should carefully take into account all above considerations when processing images of children. Children – but also older persons – should not be put in a situation in which they would, as a result of their age, be disproportionately affected by the negative consequences of facial recognition technologies. The processing needs to fully respect Article 24 (rights of the child) and Article 25 (rights of the elderly) of the Charter.

7.4. Freedom of expression and freedom of assembly and of association

The freedom of expression and information is a cornerstone of a democratic society.[146] This right is enshrined in Article 11 (1) of the Charter and in Article 10 of the ECHR. As is evident from Article 52 (3) of the Charter and the CJEU jurisprudence,[147] the meaning and scope of this right are the same as those under the ECHR, as interpreted by the ECtHR. The limitations, which may be imposed on it, may therefore not exceed those provided for in Article 10 (2) of the ECHR.[148]

Article 12 (1) of the Charter recognises and protects the freedom of assembly and of association, which corresponds to the same right enshrined in the Article 11 of the ECHR. Under Article 11 (2) of the ECHR, restrictions on this right are only allowed if these are prescribed by law, pursue one of the legitimate aims expressly listed therein (e.g. national security, public safety, prevention of crime) and are necessary in a democratic society. These limitations equally apply to the Charter right guaranteeing freedom of assembly and of association, in accordance with Article 52 (3) of the Charter.

Using facial recognition technologies to process facial images captured by video cameras in public space may interfere with a person's freedom of opinion and expression, including because a necessary aspect of exercising this freedom is group anonymity.[149] In this regard, a court in Germany declared illegal the publication of pictures taken at demonstrations via social media, due to its negative effect on the

140 Grother, P., Ngan, M., Hanaoka, K. (2019), Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification, 2019/04/12.; Galbally, J., Ferrara, P., Haraksim, R., Psyllos, Al, Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Luxembourg, Publications Office, July 2019, p. 71.

141 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, paras. 124-125.

142 FRA (2018), *The revised Visa Information System and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion 2/2018 [VIS], Vienna, 30 August 2018, pp. 67, 69.

143 CRC, Art. 8.

144 CRC, Art. 8 (2).

145 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 114.

146 ECtHR, *Mouvement Raelien Suisse v. Switzerland,* No. 16354/06, 13 July 2012, para. 48.

147 CJEU, Case C-157/14, *Société Neptune Distribution v. Ministre de l'Économie et des Finances*, 17 December 2015, para. 65.

148 *Explanations Relating to the Charter of Fundamental Rights*, OJ 2007 C 303, Explanation on Article 11, p. 21.

149 International Justice and Public Safety Network (2011), *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, 30 June 2011, p. 18.

freedom of association.[150] Knowing that people are being watched by facial recognition technologies in public spaces creates a chilling effect and may lead individuals to change their behaviour. They may not express their thoughts in the same way.[151] This infringes on their freedom of expression.

If people are discouraged to attend demonstrations, it not only goes at variance with their freedom of expression, but it also represents a serious interference with their freedom of assembly. The right of peaceful assembly enables people to participate collectively in shaping their societies in a powerful yet peaceful way. The freedom of assembly protects the ability of people to exercise autonomy while experiencing solidarity with others.[152] Using facial recognition technologies during peaceful assemblies may discourage people from demonstrating. If applied during violent protests, the technology may still affect those who protests peacefully alongside those rioting. The deployment of facial recognition technologies may generate a chilling effect whereby individuals refrain from lawfully exercising their freedom of assembly and association due to fear of the negative consequences that may follow.[153] They might thus be discouraged from meeting particular individuals or organisations, attending particular meetings or taking part in certain demonstrations. The ability to engage in these forms of activity is protected by the Charter. This chilling effect also has clear implications vis-à-vis the effective functioning of participatory democracy, and thus directly interferes with the freedom of assembly and association.[154] Civil society experts indicate that facial recognition technologies may negatively impact on the willingness of protesters to engage in activism. Hence, deploying facial recognition technology during demonstrations would need to meet an even higher threshold of necessity and proportionality than in other public spaces.

FRA highlighted that civil society organisations in some EU Member States are already highly concerned that their work is subject to state surveillance.[155] It is therefore vital that authorities are transparent about the use of facial recognition technologies and robust legislation is in place on the use of this surveillance technology.[156]

7.5. Right to good administration

The right to good administration is a well-established general principle of EU law elaborated by the CJEU and, as such, is binding all EU Member States.[157] It is also a fundamental right enshrined in Article 41 of the Charter, although only for actions of EU institutions, bodies and agencies.[158] As a general principle of EU law, it requires EU Member States to apply the requirements of the right to good administration in all public action. This right includes, but is not limited to, the right of an individual to have access to their file and the obligation of any public authority to give reasons for its decisions.[159] Access to the file facilitates understanding of the evidentiary basis on which the decision has been made, and/or of the reasons underlying it, thereby placing the individual in a better position to put forward counter-arguments when exercising the right to be heard.[160] The obligation to give reasons makes, from the perspective of the individuals affected, the decision-making process more transparent, so that the person concerned can know why a measure or action has been taken. According to the CJEU, the context in which individual decisions are made is important in determining the extent of the duty to give reasons.[161]

The right to good administration also applies when law enforcement authorities process facial images using facial recognition technologies. Although the right to good administration may be subjected to certain limitations, the question arises how to ensure

150 *Verwaltungsgericht Gelsenkirchen* (2018), 14 K 3543/18 (ECLI:DE:VGGE:2018:1023.14K3543.18.00).

151 Human Rights Council (2019), *Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, A/HRC/41/35.

152 UN, Human Rights Committee, *draft General Comment No. 37 [Article 21: right of peaceful assembly)*, draft prepared by the Rapporteur, Christof Heyns, July 2019, para. 1.

153 Fussey, P. and Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex, Human Rights Centre, July 2019, p. 36 and fn. 87.

154 *Ibid*, p. 38 and Laperruque, J. (2019), [illegible] Washington, POGO, 4 March 2019.

155 FRA (2018), *Challenges facing civil society organisations working on human rights in the EU*, Luxembourg, Publications Office.

156 See also Privacy International (2019), *Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR*, February 2019, p. 7.

157 In recent case law, see CJEU, C-604/12, *H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General*, 8 May 2014, para. 49.

158 Also confirmed by the CJEU (Joined Cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S*, 17 July 2014, paras. 66-70).

159 These components, initially developed by the CJEU case law, have been codified in Article 41 (2) of the Charter. For more on this right in leading academic literature, see Craig, P. (2014), 'Article 41 – Right to Good Administration', in Hervey, T., Kenner, J., Peers, S. and Ward, A. (eds.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford and Portland, Oregon; Hart Publishing, 2014, pp. 1069-1098.

160 *Ibid.*, p. 1082.

161 *Ibid.*, pp. 1086-1087.

that the potentially huge number of individuals have all access to their files (personal data stored). Another question is how to make sure that police and other public authorities always give reasons when someone is stopped and/or searched based on a facial recognition match.

Exercising the right to access one's file, including the personal data stored in IT systems, requires that the person is aware that their personal data are stored there. People are oftentimes not aware of the fact that their faces are recorded and processed in a database for comparison. If they are not aware of the processing, they are also not in a position to request access to their data.

Key components of the right to good administration, such as the right to access to one's file and the obligation of the administration to give reasons for its decisions, have also been translated into the more specific provisions of EU data protection law. Article 8 (2) of the Charter and the EU data protection acquis provide for the right of access, correction and deletion of one's own personal data that are stored. The possibility to exercise the right of access is part of the right to an effective remedy. If the purpose of data processing concerns 1) prevention, investigation, detection or prosecution of criminal offences, 2) execution of criminal penalties, or 3) safeguarding public security, the right to access personal data and to request the correction or erasure may be limited in the following cases according to the Law Enforcement Directive:[162]

- to avoid obstructing official or legal inquiries, investigations or procedures;
- to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- to protect public security;
- to protect national security;
- to protect the rights and freedoms of others.[163]

These exemptions stem from the obligation for law enforcement authorities to work within a certain degree of confidentiality and secrecy in order to ensure the effectiveness of their work. In this context, and as highlighted by FRA in previous reports,[164] independent accountability mechanisms are key to ensure effective access to remedies. A combination of internal and external monitoring bodies, active a different stages of the process (before, during, and after the use of facial recognition technologies) would guarantee that individuals' rights are properly and effectively protected.

According to FRA research, there is still a lack of awareness and understanding of how to exercise the right to access, correction or deletion of inaccurate personal data that are stored in large-scale IT systems.[165] The same applies to facial recognition databases used for law enforcement purposes. This situation is exacerbated by the fact that very few lawyers are specialised in seeking to enforce the right of access, correction and deletion of personal data in IT systems, including facial images used for facial recognition.

7.6. Right to an effective remedy

Article 47 of the Charter guarantees the right to an effective remedy before a tribunal, including a fair trial. This fundamental right of horizontal character empowers individuals to challenge a measure affecting any right conferred to them by EU law and not only in respect of the fundamental rights guaranteed in the Charter.[166] The right to an effective remedy also covers decisions taken with the support of facial recognition technologies, for example, a measure (such as a police stop) that has solely or significantly been informed by facial recognition.[167] The CJEU underlined that Article 47 of the Charter constitutes a reaffirmation of the principle of effective judicial protection and that the characteristics

162 Arts. 15-16.

163 See also FRA (2018), *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, p. 105.

164 See FRA (2015), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume I: Members States' legal framework*, Luxembourg, Publications Office, November 2015; and FRA (2017), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II: field perspectives and legal update*, Luxembourg, Publications Office, October 2017.

165 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 17, 100-101.

166 EU Network of Independent Experts on Fundamental Rights, *Commentary on the Charter on Fundamental Rights of the European Union*, June 2006, p. 360. See also: FRA and CoE (2016), *Handbook on European law relating to access to justice*, Luxembourg, Publications Office, June 2016, p. 92.

167 Council of Europe Commissioner for Human Rights (2019), *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, Council of Europe, Strasbourg, May 2019, p. 13.

of a remedy must be determined in a manner that is consistent with this principle.[168]

A precondition to exercise the right to an effective remedy is that a person must be aware that his or her facial image is processed. As the CJEU has noted, in the context of security measures affecting the right to private life and the right to the protection of personal data, national law enforcement authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer capable of jeopardising the investigations undertaken by those authorities.[169] Such a situation occurs, for example, when law enforcement authorities populate a 'watchlist' used for facial recognition with a great number of facial images. The CJEU has found that notification is, in fact, necessary to enable the persons affected by these measures to exercise, inter alia, their right to an effective legal remedy guaranteed in Article 47 of the Charter.[170]

EU data protection law reconfirms that the right to an effective judicial remedy must be provided in relation to decisions by the controller or the processor[171] as well as the supervisory authority.[172] Data processed by facial recognition technologies is no exception. People might want to challenge why their facial image has been included in the 'watchlist'; why it has been done so in a non-transparent way and without their consent; or seek redress for a false positive match that entailed negative consequences for them (e.g. unlawful stop, search or arrest), including seeking compensation for any damage suffered[173] (e.g. the individual missed a flight connection, or was wrongly prevented from entering an EU country and missed a business meeting).

It is crucial to note that the possibility to lodge an administrative complaint before a supervisory authority as provided for by the GDPR and the Law Enforcement Directive[174] is not considered an effective judicial remedy under Article 47 of the Charter, since no court is involved in such a review. Judicial review should always remain available and accessible, when internal and alternative dispute settlement mechanisms prove insufficient or when the person concerned opts for judicial review.[175]

168 CJEU, C-432/05, *Unibet (London) Ltd, Unibet (International) Ltd v. Justitiekanslern*, 13 March 2007, para. 37; CJEU, C-93/12, ET *Agrokonsulting-04-Velko Stoyanov v. Izpalnitelen direktor na Darzhaven fond 'Zemedelie' – Razplashtatelna agentsia*, 27 June 2013, para. 59; CJEU, C-562/13, *Centre public d'action sociale d'Ottignies-Louvain-la-Neuve v. Moussa Abdida*, 18 December 2014, para. 45.

169 CJEU, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 12. See also, mutatis mutandis, C-555/07, *Seda Kücükdeveci v. Swedex GmbH & Co. KG*, 19 January 2010, para. 52; C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 95.

170 CJEU, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 12.

171 Law Enforcement Directive, Art. 54; and GDPR, Art. 79.

172 Law Enforcement Directive, Art. 53; and GDPR, Art. 78.

173 Law Enforcement Directive, recital (88) and Art. 56; GDPR, recital (146) and Art. 82.

174 Law Enforcement Directive, Art. 52; GDPR, Art. 77.

175 Council of Europe (2019), *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), MSI-AUT(2018)06rev1, 26 June 2019, para. 4.5.

Conclusions

Using facial recognition technology – a technology that has been developing quickly in the past years and is increasingly used by multiple actors – affects a range of fundamental rights. However, there is limited information about the way and extent to which the technology is used by law enforcement, and about the impact of its use on fundamental rights. Working with new AI-driven technologies, which are not yet fully understood and where not much experience has yet been gathered, requires the involvement of all relevant stakeholders and experts from different disciplines.

Facial images constitute biometric data, EU law recognises, as they can be used to identify individuals. Facial recognition technology can be used in many different ways, such as verifying the identity of a person, checking whether a person is among a list of people, and even to categorise people according to different characteristics. Live facial recognition technology detects all faces on video footage and then compares the faces against watch lists – potentially used at public spaces.

While not much information is available about the actual use of facial recognition technology in the EU, several Member States are considering, testing or planning the use of the technology for law enforcement purposes. Most actively, the police in the United Kingdom carried out several tests in real life situations such as sports events, even using real watch lists. Other law enforcement agencies tested the accuracy of the technology in larger tests with volunteers, such as the police in Berlin, Germany or in Nice, France. The lack of more comprehensive information about the actual use of the technology limits the opportunities to analyse its fundamental rights implications. In particular, there are no laws or other guidance or information on who will be included in potential watch lists.

The fundamental rights implications of using facial recognition technology vary considerably depending on the purpose, context and scope of the use. Some of the fundamental rights implications stem from the technology's lack of accuracy. Accuracy has strongly increased, but the technology still always comes with a certain rate of error, which can negatively impact fundamental rights. Moreover, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors.

Notwithstanding the varying context, purpose and scope of the use of facial recognition technology, several fundamental rights considerations apply. The way facial images are obtained and used – potentially without consent or opportunities to opt out – can have a negative impact on people's dignity. Relatedly, the rights to respect for private life and protection of personal data are at the core of fundamental rights concerns when using facial recognition technology. In addition, any use of the technology needs to be thoroughly assessed in terms of its potential impact on non-discrimination and rights of special groups, such as children, older persons and persons with disabilities, because of the (sometimes unknown) varying accuracy of the technology for these groups and according to other protected characteristics. Moreover, freedom of expression, association and assembly must not be undermined by the use of the technology.

Lastly, the paper highlights that it is essential to consider procedural rights when facial recognition technology is used by public administrations, including the right to good administration and the right to an effective remedy and fair trial.

Given the novelty of the lechnology as well as the lack of experience and detailed studies on the impact of facial recognition technologies, multiple aspects are key to consider before deploying such a system in real life applications:

- Following the example of the large-scale EU IT systems, a clear and sufficiently detailed legal framework must regulate the deployment and use of facial recognition technologies. Determining when the processing of facial images is necessary and proportionate will depend on the purpose for which the technology is used and on the safeguards in place to protect individuals whose facial images are subjected to automated processing from possible negative consequences. Forms of facial recognition that involve a very high degree of intrusion into fundamental rights, compromising the inviolable essential core of one or more fundamental rights, are unlawful.

- A distinction must be made between the processing of facial images for verification purposes, when two facial images are compared to verify if they appertain to the same person; and their processing for identification purposes, when a facial image is run against a database or watchlist of facial images. The risk of interferences with fundamental rights is higher in the second case and therefore the necessity and proportionality test must be stricter.

- So-called "live facial recognition technologies"– when facial images are extracted from video cameras deployed in public spaces – are particularly challenging. Such a use triggers different

feelings among the population and raises fears of a strong power imbalance of the State versus the individual. These fears need to be taken seriously. Given that individuals may not be aware that their facial image is matched against a watchlist and considering the higher error rate compared to facial images taken in a controlled environment (such as an airport or a police station), their use should remain exceptional. It should be strictly limited to combatting terrorism and other forms of serious crime, or to detect missing people and victims of crime.

- When facial images are extracted from video cameras deployed in public areas, assessing necessity and proportionality of facial recognition must also consider where the cameras are placed. There is a difference between a sports or cultural event and events where people exercise one of their fundamental rights. The deployment of facial recognition technologies during demonstrations may generate a chilling effect whereby individuals refrain from lawfully exercising their freedom of assembly and association due to fear of the negative consequences that may follow. It is difficult to imagine situations where the deployment of facial recognition technologies on people participating in demonstration may be necessary and proportionate.

- Facial recognition technology algorithms never provide a definitive result, but only probabilities that two faces appertain to the same person. In the context of law enforcement, there is thus a certain margin of error leading to people being wrongly flagged. When deploying the technology, the risks of wrongly flagging people must be kept to a minimum. Everyone who is stopped as a result of the technology must be treated in a dignified manner.

- Public authorities typically rely on private companies for procuring and deploying the technology. Industry and the scientific research community can play an important role in developing technical solutions that promote respect for fundamental rights, including the protection of personal data. For this, however, fundamental rights considerations need to be built into technical specifications and contracts. The EU Public Procurement Directive (2014/24/EU) strengthened EU Member States' commitment towards a socially responsible public procurement when purchasing a product or a service. Following the spirit of the 2014 directive, the EU and its Member States could apply a similar approach when procuring facial recognition technology or commissioning innovative research. Placing fundamental rights and, in particular, data protection and non-discrimination requirements at the centre of all technical specifications, would ensure that the industry pays due attention thereto. Possible measures could include a binding requirement to involve data protection experts and human rights specialists in the teams working on the development of the technology, to ensure fundamental rights compliance by design. Furthermore, technical specifications could make reference to high quality standards to minimise false identification rates and adverse impacts on gender, ethnicity and age.

- A fundamental rights impact assessment is an essential tool to ensure a fundamental rights compliant application of facial recognition technologies, whatever the context in which it is employed. Such an assessment needs to evaluate all affected rights, including those listed in this paper, in a comprehensive manner. To enable them to carry out such assessment, public authorities need to obtain all necessary information from the industry which is required to assess the technology's impact on fundamental rights. Trade secrets or confidentiality considerations should not hinder this effort.[176]

- In light of the constantly developing technology, interferences with fundamental rights are not easy to predict. Close monitoring by independent supervisory bodies of facial recognition developments is therefore essential. Article 8 (3) of the Charter on the protection of personal data requires the oversight of data processing by an independent authority. To prevent fundamental rights violations and effectively support those people whose fundamental rights are affected by facial recognition technology, oversight authorities must have sufficient powers, resources and expertise.

176 See also Council of Europe Commissioner for Human Rights (2019), *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, Council of Europe, Strasbourg, May 2019.

Further information:

The following FRA publications offer further information relevant to the topic of paper.

- Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights (2019), https://fra.europa.eu/en/publication/2019/artificial-intelligence-data-quality
- #BigData: Discrimination in data-supported decision making (2018), http://fra.europa.eu/en/publication/2018/big-data-discrimination
- Under watchful eyes: biometrics, EU IT systems and fundamental rights (2018), http://fra.europa.eu/en/publication/2018/biometrics-rights-protection
- Fundamental rights and the interoperability of EU information systems: borders and security (2017), http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability
- The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS) (2017), http://fra.europa.eu/en/opinion/2017/etias-impact

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office of the European Union

Print: ISBN 978-92-9474-756-3, doi:10.2811/013938
PDF: ISBN 978-92-9474-758-7, doi:10.2811/52597

TK-02-19-840-EN-C (print); TK-02-19-840-EN-N (PDF)