Facial Recognition Technology and Fundamental Rights

*Michael O'Flaherty**

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'.[1]

The recent evolution of artificial intelligence (AI) powered facial recognition technology is not only attractive 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 to start using, testing or planning the use of facial recognition technologies across the world.

Examples of national law enforcement authorities in the European Union (EU) using such technology are sparse – but several are testing its potential. Most actively, and closer to home in relation to the EU, the police in the United Kingdom carried out several tests in real life situations such as sports events, even using real watch lists.[2] Other law enforcement agencies tested the accuracy of the technology in larger tests with volunteers, such as the police in Berlin, Germany[3] or in Nice, France.[4]

Using FRT 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. The lack of comprehensive and publicly available information about the actual use of the technology limits the opportu-

DOI: 10.21552/edpl/2020/2/4

* Michael O'Flaherty, Director, European Union Agency for Fundamental Rights (FRA), Vienna. For correspondence: <just_digit_secure@fra.europa.eu>.
This opinion is based on FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA focus, Publications Office of the European Union, November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 28 February 2020.

1 For more detail on how facial recognition technology works, see eg L Introna and H Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Lancaster University Management School Working Paper 2010/030, 2010) <https://eprints.lancs.ac.uk/id/eprint/49012/> accessed 28 February 2020.

2 See eg, P Fussey and D Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (University of Essex, Human Rights Centre, July 2019) <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 28 February 2020; B Davies, M Innes and A Dawson, 'An Evaluation of South Wales Police's use of Automated Facial Recognition' (Cardiff University, September 2018) <https://bit.ly/2N4Ljea> accessed 28 February 2020.

3 See eg, *Polizeipräsidium Potsdam*, 'Biometrische Gesichtserkennung' (2018) <https://bit.ly/2YgmelB> accessed 28 February 2020.

4 FRA own research, based on interviews.

nities to analyse its fundamental rights implications. In particular, there are no laws or other detailed guidance on who will be included in potential 'watch-lists'.[5]

Against this backdrop, a number of questions arise from a fundamental rights perspective: is this technology appropriate for law enforcement and border management use? Which fundamental rights are most affected when this technology is deployed? 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. All these rights are enshrined in international and regional human rights law, including the EU Charter of Fundamental Rights.[6]

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. 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. But, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors. For instance, 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. Similarly, the use of facial recognition technology can also have a negative impact on the freedom of assembly and the freedom of expression, if people fear that facial recognition technology is being used to identify them ('chilling effect'). Moreover, there are possible long-term implications. 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.

Given the novelty of the technology as well as the lack of experience and detailed studies on the human rights impact of facial recognition technologies, the EU Fundamental Rights Agency summarised, in its recent focus paper on the topic,[7] multiple aspects which are key to consider before deploying such a system in real life applications:

5 Fussey and Murray (n 2).

6 Charter of Fundamental Rights of the European Union [2012] OJ 2012 C 326/391.

7 FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA focus, Publications Office of the European Union, November 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 28 February 2020

- 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*'[8] 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*' 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;

- 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*. 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;

8 See eg, K Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779-794 <https://doi.org/10.1017/glj.2019.62> accessed 28 February 2020; M Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864-883 <https://doi.org/10.1017/glj.2019.66> accessed 28 February 2020.

- 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, 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.[9]

Working with new AI-driven technologies in the field of facial recognition technology, which are not yet fully understood and where experience of practical applications is currently limited, requires the involvement of all relevant stakeholders and experts from different disciplines. 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 EU Charter of Fundamental Rights on the protection of personal data requires the oversight of data processing by an independent authority. In the same vein, 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.

9 See also, Council of Europe Commissioner for Human Rights, 'Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation' (Council of Europe, May 2019) <https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights> accessed 28 February 2020.