**Facial recognition technology: fundamental rights considerations in law enforcement**

Rights areas:

* [Artificial intelligence and big data](https://fra.europa.eu/en/taxonomy/term/970)
* [Data protection, privacy and new technologies](https://fra.europa.eu/en/taxonomy/term/969)



Private companies and public authorities worldwide increasingly use facial recognition technology. Several EU Member States are now considering, testing or planning to use it for law enforcement purposes as well. While this technology potentially supports fighting terrorism and solving crimes, it also affects people’s fundamental rights. A new Fundamental Rights Agency’s (FRA) paper looks at the fundamental rights implications of relying on live facial recognition technology, focusing on its use for law enforcement and border management purposes.

**Publication**

[**Facial recognition technology: fundamental rights considerations in the context of law enforcement**](https://fra.europa.eu/node/37737)

FRA’s paper ‘[Facial recognition technology: fundamental rights considerations in the context of law enforcement](https://fra.europa.eu/en/publication/2019/facial-recognition)’ outlines and analyses fundamental rights challenges that are triggered when public authorities deploy live facial recognition technology for law enforcement purposes.

It identifies key aspects to consider before deploying this technology in real life:

* **Legal framework**– a clear and detailed legal framework is necessary to regulate the deployment and use of facial recognition technologies, determining when the processing of facial images is necessary and proportionate.
* **Purpose**– a distinction must be made between the processing of facial images for verification purposes and for identification purposes. In the case of identification, the risk of interferences with fundamental rights is higher. It thus requires stricter necessity and proportionality testing.
* **Impact on behaviour**– using “live facial recognition technologies” is particularly challenging because it can raise fears of a strong power imbalance of the state versus the individual. These technologies should only be used in exceptional cases, such as to combat terrorism or to detect missing people and victims of crime.
* **Place of use** – the use of facial recognition technologies during demonstrations may create a chilling effect, preventing people from exercising their freedom of assembly or association. Such use is therefore hardly proportionate or necessary.
* **Margin of error** – the algorithms never provide a definitive result, but only probabilities that two faces belong to the same person. It is therefore necessary to keep the risks of wrongly flagging people to a minimum. Moreover, anyone who is stopped as a result of using facial recognition technology must be treated in a dignified manner.
* **Public procurement** – when procuring facial recognition technologies, public authorities should build fundamental rights considerations, such as data protection or non-discrimination requirements, into technical specifications and contracts.
* **Impact assessment**– public authorities need to obtain all necessary information from the industry to carry out a fundamental rights impact assessment of the application of facial recognition technolo­gies they aim to procure and use.
* **Monitoring** – as the technology is developing fast, close monitoring by independent super­visory bodies is essential. Oversight authorities need to have sufficient powers, resources and expertise.

**Background information:**

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.

Although the accuracy of these recognition technologies 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.

Public authorities planning to use the technology in real life need to take these fundamental rights concerns seriously.