UNDER EMBARGO: 30 September 2026, 06:00 CET

FRA Press Release
Vienna, 30 September 2026

Remote biometric identification in policing: public security benefits depend on robust fundamental rights safeguards

Remote biometric identification (RBI), including facial and voice recognition technologies, supports law enforcement in preventing, detecting and investigating crime, identifying suspects and searching for victims or missing persons. But the ability to identify people remotely, including in publicly accessible places, also raises fundamental rights risks. A new report from the EU Agency for Fundamental Rights (FRA) finds that strong safeguards, effective oversight and clear legal frameworks are essential to ensure these AI-driven technologies are used lawfully and proportionately.

FRA's new report 'Remote Biometric Identification for Law Enforcement Purposes: Fundamental Rights Implications' analyses how selected EU Member States regulate and use remote biometric identification tools for law enforcement purposes.

These AI-powered technologies are currently mostly used in recorded video or audio feeds rather than in real time. The report highlights that some Member States have yet to put the necessary legal frameworks and supervisory authorities in place. While legal safeguards exist, their implementation remains uneven across EU Member States, resulting in different levels of fundamental rights protection.

FRA's research shows that measures initially introduced by governments as exceptional can become routine over time, particularly in the context of internal security policies. The report underlines the importance of putting safeguards in place before systems are deployed.

The report points to:

- **Privacy and data protection issues –** RBI systems process sensitive biometric data, often by comparing captured biometric profiles against reference databases or 'watch lists'. Their use by law enforcement including in real-time and in public spaces may affect people's private lives and interfere with their right to protection of personal data. Some

37% of people surveyed by FRA said they fear that their data could be used for unauthorised purposes.

- **Mistakes, bias and discrimination** – poorly designed and malperforming algorithmic systems can result in bias, discrimination and inaccurate biometric matches, particularly when used to identify women, ethnic minorities, children and older people. Such errors can lead to unjustified police stops and false accusations.
- **A 'chilling' effect on democratic freedoms** – 29% of the people surveyed by FRA said they would be less willing to take part in peaceful demonstrations or protests if facial recognition was used. The prospect of being identified can discourage people from exercising their rights to freedom of assembly and expression.
- **Lack of transparency and accountability** – FRA's fieldwork found limited information and transparency about the use of RBI technologies, with some Member States lacking dedicated mechanisms to inform the public about their use and operation. This makes it harder to independently scrutinise their use, identify potential misuse and challenge decisions affecting people's rights.

To ensure that RBI technologies are used lawfully and responsibly, FRA calls for:

- **Specific, effective and strict safeguards** in national laws that define clearly when and how the police can use remote biometric identification tools.
- **Protection of civic space and democratic freedoms in line with EU law** – the EU AI Act sets out a framework for the use of real-time RBI by law enforcement in public spaces. It limits its use to specific purposes, such as searching for victims or missing persons, preventing a threat to life or responding to a terrorist attack. Effective implementation requires clear national laws and consistent safeguards to ensure that these technologies are not used to identify people taking part in peaceful demonstrations or public gatherings.

Oversight and accountability – Member States must equip data protection authorities, statutory human rights bodies and other oversight bodies with the resources, powers and technical expertise needed to scrutinise these technologies, including guarding against their use beyond authorised purposes. To build public trust, law enforcement should publish the results of their fundamental rights impact assessments, going beyond what the AI Act requires. Police and technology vendors should issue regular public reports on how the tools are used.

Quote from FRA Director Sirpa Rautio:

"Public security and fundamental rights protection are not competing objectives; democracies protect people by protecting both their safety and their rights. With clear safeguards and

independent oversight, remote biometric technologies can support policing without undermining the very freedoms it is meant to safeguard. Ultimately, it is about trust. And trust is built when people are confident that these technologies are used proportionally, responsibly, and lawfully."

The report draws on research, data collection and interviews with the police, experts and the public across seven EU Member States – France, Germany, Greece, Hungary, Ireland, Italy and the Netherlands.

For more please contact: media@fra.europa.eu / Tel.: +43 1 580 30 642