

ECI Additional Information - Civil society initiative for a ban on biometric mass surveillance practices

We call on the European Commission to strictly regulate the use of biometric technologies in order to avoid undue interference with fundamental rights.

In particular, we ask the Commission to prohibit, in law and in practice, indiscriminate or arbitrarily-targeted uses of biometrics which can lead to unlawful mass surveillance. These intrusive systems must not be developed, deployed (even on a trial basis) or used by public or private entities insofar as they can lead to unnecessary or disproportionate interference with people's fundamental rights.

Evidence shows that uses of biometric mass surveillance in Member States and by EU agencies have resulted in violations of EU data protection law, and unduly restricted people's rights including their privacy, right to free speech, right to protest and not to be discriminated against. The widespread use of biometric surveillance, profiling and prediction is a threat to the rule of law and our most basic freedoms.

In this ECI, we therefore urge the Commission to propose a legal act which will build upon, and fully respect, the general prohibitions in the GDPR and the LED to ensure that EU law explicitly and specifically prohibits biometric mass surveillance.

We hereby urge the Commission to ensure that EU law explicitly prohibits biometric mass surveillance:

Our ECI calls on the Commission to permanently end indiscriminate and arbitrarily-targeted uses of biometric data in ways which can lead to mass surveillance or any undue interference with fundamental rights.

The existing EU legal framework, as it derives in particular from the GDPR and LED, clarifies that the use of biometric data shall be limited to what is strictly necessary with regards to a legitimate aim pursued, subject to the principle of proportionality. However, such general principles are subject to broad exceptions. The limited safeguards provided for by existing EU rules in their application have neither ensured transparency of biometric data processing nor prevented uses that constitute inherently disproportionate mass surveillance. Furthermore, the LED's general principles allow Member States the discretion to permit, in national law, uses of biometrics which lead to mass surveillance. This use case is in stark contradiction to Member States' obligations under EU data protection law and national constitutional protections for fundamental rights.

The EU must use its powers to prevent the transformation of all people into potential suspects subject to seamless public biometric surveillance, which undermines principles of the rule of law and purpose limitation. It must stop the abuse of biometric data which

leads to undue interference with fundamental rights and freedoms. This is key to ensure that European digital sovereignty is truly human-centric.

We urge the Commission to remedy these unlawful practices by ensuring that, based on and in full respect for the general safeguards in the GDPR and LED, EU law explicitly and specifically prohibits biometric identification, profiling and related processing or capture, in public or publicly-accessible spaces (including online), on the grounds that this leads to inherently unnecessary and disproportionate mass surveillance. The public consultation on the upcoming EU legislative initiative on AI demonstrated that there is public support for stricter regulations on uses of biometric technologies. This attention has also revealed the need for a targeted legislative proposal to ensure that Europeans' rights are sufficiently safeguarded from biometric mass surveillance.

Subject Matter

Under EU data protection law, biometric data are especially sensitive and their processing is forbidden except where there is a “substantial public interest”, subject to strict necessity and proportionality requirements. [According to a survey by the Fundamental Rights Agency](#), 83% of Europeans are against sharing their face data with authorities and 94% against sharing it with private entities.

Still, biometric data are increasingly used by national and EU law enforcement, public authorities and private entities for identification or profiling of people in public spaces. The indiscriminate or arbitrarily-targeted use of such technologies constitutes biometric mass surveillance. It poses an inherently unnecessary and disproportionate interference in a wide range of fundamental rights including privacy and data protection, and can have a ‘[chilling effect](#)’ on basic freedoms such as [expression and assembly](#). Profiling based on the processing of such data can result in [severe violations of the right to non-discrimination](#), and uses which claim to predict emotions or behaviour have [no reliable scientific foundation](#).

The EDPS has raised serious fundamental rights concerns about such technologies, calling to halt “automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals”.

Background

[Many deployments of biometric surveillance in the EU](#) have been carried out [without evidence of prior DPIAs](#), necessity and proportionality assessments or other safeguards, despite the high potential for unlawful mass surveillance and other fundamental rights abuses. [National courts](#) and [DPAs have already struck down individual deployments](#), but we need systematic action to ensure regulatory certainty.

Given the lack of awareness of the risks, the [lack of transparency in EU deployments](#) and the difficulty of enforcing the GDPR and LED's general principles, national courts and DPAs will benefit from increased legal certainty on the impermissible uses of biometric technology. Not acting risks normalising biometric mass surveillance and allowing the legalisation of national deployments for purposes which are incompatible with fundamental rights. The Commission thus faces a strong impetus to act.

The Commission's [AI White Paper](#) envisaged that, due to the risk of fundamental rights breaches, remote biometric identification should on principle be considered "high risk" and be conditional upon mandatory conformity assessments. The paper failed to fully examine the impact of such applications on fundamental rights: had it done so, we believe the only conclusion could have been that such uses ought to be considered disproportionate.

We believe that a legal act will even better protect fundamental rights if:

- It is accompanied by implementation guidance to Member States to prevent national discretion on uses that unduly restrict fundamental rights, and provide strict safeguards for all other uses in accordance with the GDPR and LED;
- The Commission ceases funding for research/development of biometric mass surveillance technologies, including for profiling, behavioural or emotional prediction;
- Member States must notify and disclose the use of any such technology to their DPA for prior assessment of legality and proportionality; and
- The AIHLEG 'Ethics Guidelines for Trustworthy AI' are encoded as the legal basis for regulating the funding of biometric technologies.

Suggested further reading & evidence

- **Ban Biometric Mass Surveillance**, EDRI, <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>
- **Use cases: Impermissible AI and fundamental rights breaches**, EDRI, <https://edri.org/wp-content/uploads/2020/09/Case-studies-Impermissible-AI-biometrics-September-2020.pdf>
- **Report on the rights to freedom of peaceful assembly and of association: The Digital Age**, UN Special Rapporteur, <https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/DigitalAge.aspx>
- **UN Special Rapporteur analyses AI's impact on human rights**, EDRI, <https://edri.org/our-work/un-special-rapporteur-report-artificial-intelligence-impact-human-rights/>
- **Facial recognition technology: fundamental rights considerations in the context of law enforcement**, EU Fundamental Rights Agency,

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

- **Your Rights Matter: Data Protection and Privacy**, EU Fundamental Rights Agency, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf
- **Data-driven policing: The hardwiring of discriminatory policing practices across Europe**, European Network Against Racism, <https://www.citizensforeurope.eu/learn/data-driven-policing-the-hardwiring-of-discriminatory-policing-practices-across-europe>