BRIEFING
STOA Options Brief

European Parliament

Person identification, human rights and ethical principles

Rethinking biometrics in the age of artificial intelligence

The policy options proposed in this briefing derive from a STOA study that explores biometrics in the era of artificial intelligence (AI) to identify the fundamental rights impact of current and upcoming developments. Taking as a starting point the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI, presented by the European Commission in April 2021, the study reviews key controversies surrounding what the proposal addresses through the notions of 'remote biometric identification' (which notably includes live facial recognition), 'biometric categorisation', and what is referred to as 'emotion recognition'. Generally speaking, the study stresses that the current legal approach to biometric data in EU law, centred on the use of such data for identification purposes, overlooks numerous present and foreseeable developments that are not centred on the identification of individuals, but would nevertheless have a serious impact on their fundamental rights and on democracy.

1. Delimiting the scope of action

1.1 Framing biometrics and biometric data

There exists no general definition of biometrics or biometric data in EU law. The proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI published by the European Commission April 2021[1] (hereafter also 'the proposed AI act' or 'the proposed AIA') reproduces the **definition of biometric data** currently found in EU data protection law ('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 data').

The definition is not particularly clear, and there is some uncertainty as to how to apply it in practice. It supports in any case a rather **narrow approach to biometric data**, qualifying as such only personal data that allow or confirm the **unique identification** of a person **through a specific technical process**. This rather narrow definition contrasts with the broader understanding of biometrics encountered in assessments of ongoing AI developments. There indeed exists broader concern regarding **AI systems that rely on the processing of data relating to the body**, data that might nevertheless not necessarily always fall under the current definition of biometric data.

It is therefore important to consider whether simply further reproducing the existing definition of biometric data in the upcoming AIA is sufficient to tackle the challenges of AI and biometrics. Crucially, it is important to see that the definitions of 'biometric categorisation' systems and 'emotion recognition' systems in the proposed AI act refer to the processing of biometric data, meaning that their scope is thus **indirectly circumscribed and affected by the narrow and not fully clear definition of biometric data described above**.

1.2 An improved path to the qualification of AI systems as high risk

The procedure envisaged by the proposed AI regulation **to add types of AI systems to the list of AI systems regarded as 'high risk'** gives a prominent role to the European Commission, without detailing with sufficient clarity how such a procedure would unfold, how to initiate it or request its launch, or how long it could take. Furthermore, the procedure envisaged rests on an ultimately subjective appreciation of whether the AI systems to be added to the list might have an **equivalent or greater adverse impact on fundamental rights** compared with the adverse impact initially included in the list.

In order to prevent the irreparable materialisation of an adverse impact on fundamental rights, it is crucial to design a robust and open system for the inclusion of new categories of AI systems on the list of high-risk systems. Provision must be envisaged for a **faster**, **clearer** and **accessible path** for qualifying additional AI systems as high-risk systems. **Civil society organisations** could be given a role to raise the alarm of major risks, not least since the persons affected would potentially be in vulnerable positions, and might not be easily able to document and communicate harms by themselves.

2. Remote biometric identification

2.1 A real and unambiguous ban

The proposed AI regulation fails to prohibit real-time remote biometric identification in public spaces for law enforcement purposes. What it provides for is actually **a framework to allow for the widespread use of such AI systems**. This approach does not effectively prevent **the serious adverse impact that could stem from the deployment in Europe of an infrastructure allowing for the recurrent** – even if recurrently short-term – **authorisation of remote biometric identification in public spaces for law enforcement purposes**.

In particular, the **persistent tracking of individuals in public spaces by means of remote biometric identification**, whether or not for law enforcement purposes, **must be explicitly and unambiguously prohibited**, as it would have major consequences for fundamental rights and democracy as such.

2.2 'Post' remote biometric identification

In relation to remote biometric identification, the proposed AI regulation fails to address properly the risks connected to the **retroactive identification** using facial recognition of individuals whose images have been recorded while they were in public spaces – it does not even formally prohibit the **'post' remote biometric identification of natural persons**, which is deemed as falling under the high-risk category of AI systems, and thus potentially subject to certification.

In practice, the **risk of persistent tracking and its associated adverse impact on fundamental rights and democracy** are, however, at least equivalent. 'Post' remote biometric identification of natural persons recorded while in public spaces should be subject to the same rules as the 'real time' equivalent.

2.3 Safeguards for any remote biometric identification

The proposed AI regulation leaves it up to the Member States to define by law the exact conditions for the use of real-time remote biometric identification in public spaces for law enforcement purposes, which is in principle prohibited but actually permitted. The only detailed condition is the need for **prior authorisation** granted by a judicial authority or by an independent administrative authority (proposed article 5(3) AIA).

Experience has shown that when the EU legislator adopts legislation that establishes limitations of fundamental rights while referring to necessary safeguards to be adopted later at national level, **serious problems can emerge**. A similar lack of specified safeguards led to the invalidation of the Data Retention Directive.[2]

Substantive safeguards for prohibited but exceptionally permitted uses of real-time remote biometric identification, if any, must be specified at EU level in the future AIA itself, as opposed to being left to the discretion of the Member States.

3. Other AI systems defined with reference to biometric data

3.1 AI systems assigning individuals to sensitive categories

The proposed AI regulation gives a definition of a 'biometric categorisation system' that is not only **unclear** but also **conceptually problematic**, most notably to the extent that it seems to endorse that it is possible – scientifically, ethically, legally – to use AI systems to assign natural persons to a sexual orientation or to a political orientation. If a reference to the use of similar AI systems persists in future versions of the proposal, it should be phrased clearly as **a prohibition**.

The question of the definition of biometric data is crucial when it comes to properly assessing the potential impact of such a ban on current and future problematic practices. It is therefore necessary to assess whether certain AI systems that categorise individuals should be prohibited **regardless of whether they categorise on the basis of biometric data**.

3.2 'Emotion recognition'

The status of 'emotion recognition' in the proposal for a regulation on AI is **not entirely clear**. The proposed definition of emotion recognition seems to imply that emotions and intentions of individuals can be inferred **from biometric data**. This could only possibly make sense if biometric data were understood in a broad sense, not limited to data allowing for the unique identification of individuals. In addition, the list of high-risk systems in Annex III includes various references to **systems used 'to detect the emotional state of a natural person'**, without clarifying if these would correspond to what is defined as 'emotion recognition' systems or would potentially be something else.

4. Effective rights and justified exemptions

4.1 Increase transparency towards individuals

Generally speaking, the proposed AI regulation privileges imposing obligations on **actors other than the users of AI systems**, who are subject to a limited number of provisions only. The use of extremely high-risk systems in particular should be conditioned on **additional obligations imposed on users towards individuals**, notably in terms of transparency both prior to use and during use. Transparency is crucial for the exercise of rights and the effectiveness of remedies, which must be duly provided. Limitations to transparency should be compensated with measures that guarantee the accountability of such limitations.

4.2 No special exemptions for large-scale EU databases

The use of biometrics and AI in EU large-scale information technology (IT) systems is massive, raising serious risks for fundamental rights. It is **of great concern** that the European Commission's proposal for a regulation on AI deliberately pushes away from its scope of application certain AI systems to be used in the context of the Schengen information system (SIS), the Visa information system (VIS), Eurodac, the entry/exit system (EES), the European travel information and authorisation system (ETIAS),

the European criminal records information system on third-country nationals and stateless persons (ECRIS-TCN), and their interoperability.

More specifically, proposed article 83(1) AIA would leave out of its scope in an indefinite manner any AI system used in such a context if the AI system was put on the market at any moment during the first year of application of the proposed regulation. This could have as an indirect effect **to incentivise a major advent on the market of potentially high-risk systems** that will nonetheless manage to evade the need to comply with the regulation, later **to be used in systems that process massive quantities of sensitive data of individuals often in a vulnerable position**. This must be avoided. It is essential that large-scale IT systems in the area of freedom, security and justice (AFSJ) fully comply with the highest standards of EU law.

NOTES

1 European Commission, proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final, Brussels, 21 April 2021.

2 *Digital Rights Ireland Ltd*, 2014; CJEU Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

This document is based on the STOA study 'Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence'. The study was written by Professor Gloria González Fuster and Michalina Nadolna Peeters of the Law, Science, Technology and Society (LSTS) Research Group at Vrije Universiteit Brussel (VUB) at the request of the Panel for the Future of Science and Technology (STOA), and managed by the Scientific Foresight Unit, within the Directorate General for Parliamentary Research Services (EPRS), European Parliament. STOA administrator responsible: Mihalis Kritikos.

DISCLAIMER AND COPYRIGHT

stoa@ep.europa.eu (contact)

http://www.europarl.europa.eu/stoa/ (STOA website)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)