Ref. Ares(2021)5674926 - 16/09/2021

European Commission

Rules on biometrics in the AI proposal

Consistency with the existing legal framework

Legal basis: Art. 16 TFEU “Data protection”

Consistency is ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality.

The proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development, use and transparency of certain AI systems processing biometrics and restrictions on the use of real-time remote biometric identification systems.

It constitute a lex specialis to Art. 10 LED. The AI Regulation does not specify and prohibit use cases falling under Art. 9 GDPR.

It is without prejudice to the legal framework of SIS.

European Commission

Regulation of biometrics – product and use

Biometric identification and categorisation of natural persons (Annex III (1))

- **Products qualify as high risk**
- **Products limited to** AI systems intended to be used for the **'real-time' and 'post' remote biometric identification** of natural persons;
- Ex-ante third-party conformity assessment

Biometric categorisation and emotion recognition (Art. 52 (2))

- Harmonised transparency rules for the **use**
- **Mandatory information** of the person exposed to such system
- **Exception for law enforcement**: no need to inform the person in case of biometric categorisation

Real time remote biometric identification in publicly accessible places (Art. 5 d))

- general prohibition for law enforcement with exceptions as a lex specialis to Art. 10 LED
- Other users must apply the GDPR containing a prohibition with exceptions

European Commission

Definitions (1)

- ‘biometric data’ means 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;
- ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;
- ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

Real-time remote biometric identification

European Commission

Definition (2)

- ‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;
- ‘‘real-time’ remote biometric identification system’ means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.
- ‘‘post’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;
- ‘publicly accessible space’ means any physical place accessible to the public, regardless of whether certain conditions for access may apply;

Scope

Remote biometric identification: 1) real time (fixed terminals, mobile terminals, drones)

2) post-processing of facial images captured remotely and comparing them to reference database (CCTV, bodycams, mobile phones)

Out of scope of the AI Regulation but subject of LED:

a) identity checks carried out for law enforcement, border and other security purposes (booths, ABC-gates, mobile devices, police stations, entrance of venues)

b) social media comparison (Clearview)

c) examination of images held in electronic devices

Publicly accessible place

For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned.

- Public spaces
- Spaces open to the public (shopping malls, banks, public parking, airport entry halls, public transport, etc)
- Stadiums and other venues

Not covered: places that are private in nature and normally not freely accessible for third parties; police/border identity check at the entry (white&black lists)

Real time biometric identifications – subject matter of the regulation

The overall applicable legal framework consists of the national laws transposing LED, the AI Regulation and the specific laws to be adopted based upon the AI Regulation. The regulation altogether consists of three layers:

1) Real time RBI products are subject of an ex-ante third-party conformity assessment (provider)
2) Deployment of the real-time RBI system requires a data protection impact assessment and the authorization of DPA (user)
3) Use of the real-time RBI system is subject of strict conditions laid down in national laws based upon the AI Regulation (user)

Use of real time biometric identifications – layered approach

General prohibition only for law enforcement – use is allowed under multiple consecutive conditions:

1) The AI legislation does not constitute a legal base but only provides a framework beyond which such system can be implemented
2) National law is required but Member States can also decide not to regulate it
3) Activation only to fulfil one of the three objectives
4) Ex-ante authorization of the judiciary or an independent administrative body to activate the system
5) Confirmation of hits by two experts

European Commission

Real time biometric identifications – objectives

General prohibition unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific potential victims of crime, including missing children (can include trafficking victims or missing persons where crime cannot be excluded);

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack*; (N.B. it can also include vulnerable missing persons who urgently need medication)*

(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. *(N.B. it does not require the issuance of an EAW; in case of a serial offender points ii) and iii) can be referred to)*

European Commission

Authorisation of real time biometric identification

1) To issue by a judicial authority or independent administrative authority
2) Ex-ante but exceptionally it can be ex-post (in case of a duly justified situation of urgency
3) To base on objective evidence or clear indications presented to it, that the use is necessary for and proportionate to achieving one of the objectives
4) To weight – (i) the situation (seriousness, scale of harm, probability of occurrence)

   (ii) impact on fundamental rights

5) Appropriate safeguards including the conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations

Other conditions

1) Record keeping in the form of logging:

a) recording of the period of each use of the system (start date and time and end date and time of each use);

b) the reference database against which input data has been checked by the system;

c) the input data for which the search has led to a match;

d) the identification of the natural persons involved in the verification of the results

2) Human oversight

Thank you

European Commission