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

European Commission

Rules on law enforcement, migration and asylum in the AI proposal

Objectives of the Commission in relation to home affairs

- to ensure a nuanced approach, namely that not all AI applications are considered automatically **high risk** in home affairs but only those which would fall under the criteria;
- to maintain to the possible extent the existing national powers of law enforcement and the relevant national laws when using facial images as a **biometric identifier** for investigations;
- to set up tailor made **procedures** for law enforcement and border security to safeguard public security and the secrecy of investigations by limiting disclosure and transparency of the AI applications they use;
- to decrease administrative burden on home affairs authorities in order not to hamper **innovation and in-house developments**;
- to ensure that the implementation of the EU large-scale IT systems for migration, border management and security are not delayed.

General scope of the AI proposal

- The AI proposal has a horizontal scope, with the exception of AI application exclusively for military use (not the dual use products).
- It determines prohibited AI applications (Art. 5).
- It determines rules applicable for the development and throughout the life-cycle of AI application, which qualify as high risk serving:

  a) biometric identification or categorisation of natural persons

  b) law enforcement

  c) migration, asylum and border control management

- It determines substantial rules concerning the use of certain AI application:

  a) real-time biometric identification (Art. 5 (d))

  b) chatbots and biometric categorisation (Art. 52 (1) and (2))

  c) deep fakes (Art. 52 (3))

European Commission

Personal scope

1) Personal scope: operators, i.e. providers, importers, distributors, authorised representatives and users:

2) ‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

3) ‘user’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

4) More specifically:

- Private businesses as provider (maybe as user too under certain circumstances)
- End-users (law enforcement, asylum authorities, border control agencies, etc) as provider and user
- JHA Agencies

European Commission

Law enforcement according to LED

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(c) 'law enforcement' means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

Who are they? It is determined under national law but typically

- Customs and tax authorities
- Municipalities, public transport companies or prisons

European Commission

Territorial scope – extraterritorial effect

EU territory (Art. 2 (1) (a), (b), (c)

(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;

(b) users of AI systems located within the Union;

(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union;

Exception (Art. 2 (4)): no application to public authorities in a third country nor to international organisations, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States

Date of application

Date of application is 24 months following the entry into force, except the penalities, which already apply after 12 months and setting up the notifying and notified bodies (Title III Chapter 4) and the overall governance (Title VI), which will apply after 3 months.

1) No retroactive effect: no application to the high-risk AI systems that have been placed on the market or put into service before [date of application], only if, from that date, those systems are subject to significant changes in their design or intended purpose.

2) Special provisions for the large-scale IT systems: application only to those AI components of the large-scale IT systems that have been placed on the market or put into service before 36 months after the entry into force, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned; the periodical review of the legal bases of the systems will take into account the necessary alignment with the AI Reglation.

High risk applications for law enforcement

Main areas:

a) Risk assessment of persons and groups and prediction of their behaviour

b) Processing of personal data for profiling in accordance with the LED definition:

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

d) Deep fakes

e) Big data analysis

f) Evaluation of evidence

Annex III point 6 (1)

(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;

(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

Annex III point 6 (2)

(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

High risk applications for migration, asylum and border control management (Annex III point 7)

a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

Low-risk AI systems in migration

	Low risk	Why
1	AI systems that inform the applicant/traveller of applicable conditions – So-called chatbots	If the information would be wrong/biased etc.. the applicant/traveller will "only" be disappointed when his/her application needs to be corrected. It is in the interest of the authorities to provide correct information as otherwise it will have too much re-work. Chatbots are intended for border control, visa applications, travel authorisations, applications for residence permits.
2	AI systems for triaging of cases according to the work distribution within the administration.	If the triaging would be wrong, official would receive cases that do not match their experience, interest, capacities. They would re-direct the cases manually. It is in the interest of authorities to allocate cases correctly and avoid re-assignments. Triaging systems are intended for border control, visa applications, travel authorisations, residence permits.
4	AI systems for identifying the risk indicators. The individual risk evaluation is however high-risk as mentioned in the text of the Annex II	Risk indicators are identified on the basis of the analysis of potentially the complete set of cases. AI would be expected to help identify risk patterns out of such large datasets. If the risk indicators are badly identified it leads to non-meaningful case selection. The administration must select properly. There is a comparison that can be done between identified cases without and with AI.
5	AI systems for establishing country and route specific risks	This follows from 5. What are the specific risks for given countries and travel routes. It does not target persons individually but the context that makes a given origin or route subject to check more persons than on low-risk routes. If the tool works badly the checks will be done on the persons on the wrong routes.
6	AI systems for allocation of resources according to the expected number of border crossings	This is a tool for achieving a better estimation of required resources. If working wrongly resources are wrongly allocated.
7	AI systems for performing a situational awareness	This is a means for supporting the analysis where bottlenecks, crisis situations are likely to happen. If working wrongly the situational awareness does not prepare for the bottlenecks, crisis situations where they occur.

Obligations for providers

(a) ensure that their high-risk AI systems are compliant with the requirements

(b) have a quality management and a risk management system as well as an accountability framework. For national authorities these can be established at national or regional level.

(c) draw-up the technical documentation of the high-risk AI system;

(d) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(e) comply with the registration obligation in the EU database; instructions do not need to be published for home affair systems;

(f) transparency requirements in form of instructions for the users;

(g) affix the CE marking to their high-risk AI systems to indicate the conformity with the AI Regulation;

(h) Log keeping, corrective measures, etc.

Ex-ante competent authorities

Ex ante conformity assessment for remote biometric identification systems:

- High risk AI systems for remote biometric identification require a third-party conformity assessment for the providers.
- A third party approval is also required to set up the quality and risk management framework.
- Exception: if the remote biometric identification system is based upon harmonised standards the conformity assessment will be conducted as an internal control.
- In case the provider is a private business the competent authoritiy is the notified body.
- In case the provider is a law enforcement, migration or asylum authority the competent authority is the data protection authority.
- In case the provider is a JHA agency the competent authority is EDPS.

Ex-ante competent authorities

Ex ante conformity assessment for other high risk AI applications (Annex points 6 and 7):

- High risk AI systems require an internal control procedure (Art. 43 (2)).
- No third party approval is required to set up the quality and risk management framework.

Obligation of the users

(a) ensure that their high-risk AI systems is used according to the instructions;

(b) implement the human oversight measures to ensure the transparency and explainability requirements

(c) exercises control over the input data, in particular ensures that input data is relevant in view of the intended purpose of the high-risk AI system

(d) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(e) Carries out a data protection impact assessment if applicable;

(f) Log keeping, monitoring, corrective measures, etc.

Ex-post monitoring: market surveillance

- Providers (i) must establish a post market monitoring framework and a monitoring plan

  (ii) must give access to data, the documentation and the source code

  (iii) must notify serious incidents

- Users: must regularly inform the providers about the functioning of the system

European Commission

Ex-post Competent authorities

Market surveillance authorities for the purposes of high-risk AI systems (Annex points 1, 6 and 7) when they are used for law enforcement migration and asylum purposes are:

- data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems
- EDPS in case of such systems operated by the JHA Agencies.

European Commission

Confidentiality obligation

- National competent authorities and notified must respect the confidentiality of information and data obtained in carrying out their tasks and activities in including the integrity of criminal and administrative proceedings.
- Requirement of a security clearance.
- Information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardise public and national security interests.

European Commission

Exceptions for law enforcement from the transparency obligations

General obligation to inform persons that they interact with AI systems with the exception if such system is used for law enforcement purposes:

(i) Chat bots

(ii) Deep fakes: users of AI systems generating manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful must inform the persons affected.

It will not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.

(iii) Biometric categorisation

Regulatory sandboxes (Art. 53, Art. 54)

- a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan
- Under the direct supervision of the national competent authorities
- Specific provision to repurpose the use of personal data under strict condition in line with Art. 6 (4) GDPR:

“the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law”

Thank you

European Commission