Rules on migration, asylum and border management in the AI proposal

DG HOME

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 by the alignement with the existing regulatory procedures (DPIA)**;
- to ensure that the implementation of the **EU large-scale IT systems** for migration, border management and security are not delayed.

Exceptions from the scope of the AI proposal

The AI proposal has a horizontal scope for public and private entities, with a global approach, with the following exceptions:

a) AI application exclusively for military use (not the dual use products, such as UAS, object recognition, maritime surveillance);

b) AI applications and their use for national security

c) third-country law enforcement, judiciary and international organisation when they are acting on the basis of international agreements

General scope of the AI proposal

- It determines rules applicable for the AI products concerning 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

Sector based approach

- Sensitive areas are listed and can be only changed with an amendment to the legislation.
- Consequence is a double standard: the same application can be low and high risk depending if it falls under any of the sectors.

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

European Commission

Significance of AI border security and border management

- Automated border checks (identification of persons, verification of travel documents
- Algorithmic recognition and classification of objects (e.g. customs checks)
- Maritime domain awareness
- Unmanned surveillance capabilities
- Predictive analytics
- Geospatial data analytics

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: no application 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.

Definition and technological scope of the regulation (Annex I)

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

Not only self-learning and autonomous systems but also rule based systems (expert systems) and statistical analytical systems are also captured, which means that also pure automation of processes and tasks may fall under the proposal (CRRS)

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

No matter if the data is personal or non-personal data, which is used to train the AI system as the criteria to be looked at is an impact on fundamental rights of the individual to which the AI system applies.

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.

European Commission

Emotion recognition

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

- Hypothetical case as it is not applied in practice (H2020 iBorderCTL research project)
- Such method can be used in any stage of the procedure be it on EU territory, at the external border or in third-countries, such as visa application process, asylum application or an interview at the regular border crossing point
- Third-country national and EU citizens

European Commission

Individualised risk assessment systems

- 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
- ETIAS, API-PNR, VIS;
- Third-country national and EU citizens
- Q1: if AI tools for customs check of personal belongings could qualify for this purpose (object recognition or recognition of endangered species)?
- Q2: Could AI tools for the analysis of the media of an irregular migrants qualify as high risk in this context?

European Commission

Security features of documents

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;

- Scope extends not only to personal identification documents but also to breeder documents (ongoing research on AI to verify the authenticity of breeder documents)
- Such AI tool can be foreseen at any stage of a procedure (i.e visa application, border checks including eGates, asylum process or residence status)
- Q1: Would the detection of spoofing and morphed images also fall under this category?

European Commission

Examination of asylum application, visa and resident permits

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.

- Dialect recognition tools
- Scoring tools showing the level of integration (not used in the EU)
- It does not include chatbots, workflows, case allocation systems or other administrative assistant systems

European Commission

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.

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.

Rules on biometrics in the AI proposal

DG HOME

Scope – Relation to SIS and the future Prüm

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

c) examination of images held in electronic devices

European Commission

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

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)

Thank you

© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the CC BY 4.0 license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Slide xx: element concerned, source: e.g. Fotolia.com; Slide xx: element concerned, source: e.g. iStock.com

European Commission