Annex - Detailed recommendations

In order to achieve the calls outlined in the civil society statement 'EU policymakers – regulate police technology!', the EU AI Act must:

1. Include legal limits prohibiting AI for uses that pose an unacceptable risk for fundamental rights. This includes a legal prohibition on different forms of biometric surveillance, predictive policing, and harmful uses of AI in the migration context.

- A full ban on real-time and post remote biometric identification in publicly accessible spaces (including border areas and around migration detention facilities), by all actors, without exception (Article 5(1)(d));
- A broad definition of of public-accessible spaces, which includes border areas (Reject Recital 9, Council Mandate);
- A prohibition of all forms of predictive and profiling systems in law enforcement and criminal justice (including systems which focus on and target individuals, groups and locations or areas) (Article 5(1)(da) EP mandate);
- Prohibitions on AI in migration contexts to make individual risk assessments and profiles based on personal and sensitive data, and predictive analytic systems when used to interdict, curtail and prevent migration;
- A ban on the use of biometric categorisation systems, such as racial, political or gender profiling systems (Article 5(1) (ba) EP mandate) ;[1] and the use of automated behavioural detection systems in publicly accessible spaces; [2]
- A ban on the use of so called 'emotion recognition' systems to infer or predict people's emotions and mental states[3]
- Prohibit export of systems which are banned in the EU (article 2(1) of the European Parliament mandate).

2. Provide public transparency and oversight when police, migration and national security agencies use 'high-risk' AI, by upholding an equal duty of these authorities to register high risk uses in the EU AI database.

---

1 EP mandate: Article 5.1.(ba) – ban on biometric categorisation, but limited to characteristics defined in recital XX.

2 EP: ban on automated behavioural detection received strong support in Plenary but did not make the final text.

3 EP mandate: Art. 5.1.(d)(dc) – ban on emotion recognition in specific sectors: law enforcement….

- Uphold the obligation to register themselves and their use of AI high-risk systems in the public database (Reject exemption foreseen in Articles 29 (5) and 51 (2);
- Require equal transparency for providers of high-risk systems deployed in the areas of law enforcement and migration to register their products on the public database (Reject exemption foreseen in Article 51 (1) Council mandate);
- Ensure the reporting of the testing of AI systems in sandboxes is transparent and no blanket exemption is made for processing of 'sensitive operational data' , which is a vague and broad term (Reject exemptions foreseen in Articles Article 53 (5), Article 54 (1) (j));
- Ensure the obligation to register the testing in real-world conditions in the EU database (Reject exemptions foreseen in Articles Article 54a (4) (c) and 54a (4) (j) Council mandate);
- Ensure strong human oversight measures apply consistently throughout the Act, especially for AI high-risk systems used by these authorities (Reject exemptions foreseen in Articles 14(5) and Article 29 (4)).

3. Ensure that the AI Act properly regulates the uses of AI in policing, migration and national security that pose risk to human rights, specifically a comprehensive list of AI in migration control, and ensuring that national security is not excluded from scope.

- Reject the Council's addition of a blanket exemption from the AI Act of AI systems developed or used for national security purposes (Article 2(3) Council mandate);

  Reject the blanket exemption for high-risk systems that are part of migration databases (e.g. EURODAC, VIS, SIS) listed in Annex IX (as per Article 83(1) EP Mandate);
- Ensure the list of high-risk systems in Annex III includes all potential dangerous AI systems:
  - BIometric identification systems, such as hand-held facial image, fingerprint or palm scanners, voice or iris identification technology, whose use can lead to discrimination, surveillance and coercion of the person subjected (Annex III, Point 1 EP Mandate)
  - AI systems used for border management activities, such as unmanned drones or thermal cameras, which can lead to the violent interception of asylum seekers and their push-back (Annex III, Point 7 (d a) EP Mandate);
  - AI systems to forecast migration movements and border crossings whose use can inform punitive policies (Annex III, Point 7 (d b) EP Mandate).