A dangerous precedent: how the EU AI Act fails migrants and people on the move

On 13th March 2024, the EU Artificial Intelligence Act (AI Act) was adopted by the European Parliament. Whilst the legislation is widely celebrated as a world-first, the EU AI Act falls short in the vital area of migration, failing to prevent harm and provide protection for people on the move.

In its final version, the EU AI Act sets a dangerous precedent. The legislation develops a separate legal framework for the use of AI by law enforcement, migration control and national security authorities, provides unjustified loopholes and even encourages the use of dangerous systems for discriminatory surveillance on the most marginalised in society. This statement outlines the main gaps in protection with respect to AI in migration.

Why the EU AI Act fails migration

The EU AI Act seeks to provide a regulatory framework for the development and use of the most 'risky' AI within the European Union. The legislation outlines prohibitions for 'unacceptable' uses of AI, and sets out a framework of technical, oversight and accountability requirements for 'high-risk' AI when deployed or placed on the EU market.

Whilst the AI Act takes positive steps in other areas, the legislation is weak and even enables dangerous systems in the migration sphere.

- **Prohibitions on AI systems do not extend to the migration context.** The legislation introduces (limited) prohibitions for harmful AI uses. EU lawmakers refused to ban harmful systems such as discriminatory risk assessment systems in migration and predictive analytics when used to facilitate pushbacks. Further, the prohibition on emotion recognition does not apply in the migration context, therefore excluding documented cases of AI lie detectors at borders.

- **The list of high-risk systems fails to capture the many AI systems used in the migration context** and which, eventually, will not be subjected to the obligations of this Regulation. The list excludes dangerous systems such as biometric identification systems, fingerprint scanners, or forecasting tools used to predict, interdict and curtail migration.

- **AI used as part of EU large-scale databases** in migration, such as Eurodac, the Schengen Information System, and ETIAS will not have to be compliant with the Regulation until 2030.

- **Export of harmful surveillance technology:** the AI Act did not address how AI systems developed by EU-based companies impact people outside the EU, despite existing evidence of human rights violations facilitated by surveillance technologies developed in the EU in third countries (e.g., China, Occupied Palestinian Territories). Therefore, it will not be prohibited to export a system banned in Europe outside of the EU.

A dangerous precedent: enabling harmful surveillance by police and migration authorities

Perhaps the most harmful aspect of the EU AI Act is the creation of a parallel legal framework when AI is deployed by law enforcement, migration and national security authorities. As a result of pressure exerted by Member States, law enforcement and security industry lobbies, these authorities are explicitly exempted from the most important rules and safeguards within the AI Act:

- **Exemptions to transparency and oversight safeguards for law enforcement authorities.** The Act introduces transparency safeguards requiring public authorities using high-risk AI systems to register information about the system onto a publicly accessible database. The AI Act introduces an exemption to this requirement for law enforcement and migration authorities, instilling secrecy for some of the most harmful AI uses. This will make it impossible for affected people, civil society and journalists to know where AI systems are deployed.

- **The exemption on national security** will allow member states to exempt themselves from the rules for any activity they deem relevant for "national security", in essence a blanket exemption to the rules of the AI Act which could in theory be used in any matters of migration, policing and security.

These exemptions effectively codify impunity for the unfettered use of surveillance technology, setting a dangerous precedent for the use of surveillance technology in the future. In effect, AI Act lawmakers have vastly limited crucial scrutiny of law enforcement authorities and have enabled more and more use of racialised and discriminatory surveillance. First and foremost, these loopholes will harm migrants, racialised and other marginalised communities who already bear the brunt of targeting and over-surveillance by authorities.

Fundamental rights, surveillance tech and migration: what's next?

The EU AI Act will take between 2-5 years to enter into force. In the meantime, harmful AI systems will continue to be tested, developed and deployed in many areas of public life. Furthermore, the EU AI Act is only one legal context in which the EU is enabling surveillance technology. From the

Screening Regulation, Eurodac, to many others, we see an expanding legal framework that surveils, discriminates against and criminalises migrants.

The #ProtectNotSurveil coalition started in February 2023 to advocate for the AI Act to protect people on the move and racialised people from harms emanating from the use of AI systems. This coalition will continue to monitor, advocate and organise against harmful uses of surveillance technology. Crucial next steps will be:

- For EU and national level bodies to document and respond to harms stemming from the use of AI in migration and policing contexts, ensuring protection against the violation of peoples' rights.
- For civil society to contest further expansion of the surveillance framework, reversing and refusing trends that criminalise, target and discriminate against migrants, racialised and marginalised groups.
- For all to re-evaluate the investment of resources in technologies that punish, target and harm people as opposed to affirming rights and providing protection.

The #ProtectNotSurveil coalition

Access Now, European Digital Rights (EDRi), Platform for International Cooperation on Undocumented Migrants (PICUM), Equinox Initiative for Racial Justice, Refugee Law Lab, AlgorithmWatch, Amnesty International, Border Violence Monitoring Network (BVMN), Digitalcourage, EuroMed Rights, European Center for Not-for-Profit Law (ECNL), European Network Against Racism (ENAR), Homo Digitalis, Privacy International, Statewatch, Dr Derya Ozkul, Dr. Jan Tobias, and Dr Niovi Vavoula