Regulating AI at Europe's Borders

Where the AI Act Falls Short

Niovi Vavoula

13.12.2024 doi: 10.59704/10a27137a898fa42

Introduction

The adoption of the AI Act constitutes a pivotal moment in the regulation of AI systems deployed in the EU, including the field of migration, asylum and border management. This blog aims to provide a concise analysis of the immigration-related provisions, arguing that the classification of the high-risk AI systems is particularly problematic and that the various exceptions and gaps of the AI Act safeguards applicable in this field will amplify the fundamental rights challenges and create accountability gaps.

The Problematic Classification of High-Risk AI Systems

In the field of migration, asylum and border management, where decision-making is highly discretionary and discrimination between citizens and non-citizens is inherent in the very nature of this field of law, AI can revolutionise the way states manage mobility, decision-making, and community integration. AI promises modernised border controls, as well as expedited decision-making in relation to applications for visas, residence permits, travel authorisations or asylum through algorithmic risk assessments. Various AI systems are already piloted, developed or implemented in EU Member States individually and as whole: tools that verify the authenticity of documents provided by foreigners; tools for the recognition of emotion, such as the IBorderCntrl project or speech to test the veracity of applicants' claims; or systems that perform risk assessments based on personal data provided by the foreigners concerned. AI tools may also be used for more evidence-based policy-making based on predictive analytics; or for enhanced situational awareness in border regions (for example, see here).

AI can promote neutrality, objectivity, and standardisation in decision-making, thus potentially decreasing discriminatory treatment of third-country nationals. However, it also poses significant risks for the protection of fundamental rights, such as non-discrimination, due to biases in the design or implementation of the algorithms, and effective remedies. In this field, the challenges are more acute considering that the targeted individuals are in a weaker position than EU citizens.

Recital 39 AIA recognises the AI systems in this field "affect persons who are often in particularly vulnerable positions and who are dependent on the outcome of the actions of the competent public authorities". Yet the AI Act does not envisage the prohibition of any AI system and instead, Annex III classifies as high-risk the four AI systems below:

(a) polygraphs or similar tools;

(b) for assessing a risk posed by a person who intends to enter or who has entered into the territory of a Member State;

(c) to assist in the examination of applications for asylum, visa or residence permits, including assessments of the reliability of evidence; and

(d) for detecting, recognising or identifying persons, including autonomous surveillance towers fielded in border regions with surveillance capabilities to detect irregular border crossings or Automatic Identification Systems (AIS) used for maritime awareness and surveillance, except for the verification of travel documents.

This classification is problematic, as not only certain AI systems have been *wrongly classified* but also because the list of high-risk AI systems is *incomplete*. The most prominent example of incorrect classification is emotion recognition systems based on scientific

theories of dubious validity. Such systems include lie detectors that infer emotions based on biometric data and behavioural analytics which detect "suspicious" individuals based on how they look. I argue that all emotion recognition should have been banned under Article 5 of the AI Act; considering that emotions gain meaning through culture, are not uniform across societies, emotion recognition systems are unreliable, and there exists no link between facial expressions and inner emotional states. In the field of migration in particular, their use will reinforce a process of racialised suspicion towards third-country nationals and can automate discriminatory assumptions.

Furthermore, there is a significant gap in the list of high-risk AI systems, specifically for those that involve predictive analytics. This is notwithstanding the European Parliament's efforts to classify AI systems "for the forecasting or prediction of trends related to migration movement and border crossing" as high risk. By predicting the arrivals of migrants in any given state, these systems can influence efficient preparedness for increased arrivals of people and enable the reallocation of resources depending on reception needs. However, predictive analytics may also facilitate preventive responses to halt movement, for example through pushbacks or by recruiting third countries as the gatekeepers of EU borders.

Biometric identification is not subject to tailor-made rules in the field of migration, asylum and border management. Annex III of the AI Act allows the deployment of AI systems for biometric identification that would scan border areas to deter and prevent migrants from entering and seeking international protection and classifies them as high-risk. The need for tailor-made rules would have been important to acknowledge the significant risks of discrimination, as they can facilitate and increase the unlawful practice of racial profiling by using ethnicity or skin colour as proxies for an individual's migration status. In turn, biometric verification systems are considered of limited risk. Besides, biometric verification also presents risks for discriminatory treatment. As for "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, this is prohibited, subject to three exceptions. These are: if "the targeted search for specific victims of abduction, trafficking in or sexual exploitation of human beings, as well as the search for missing persons' or for "the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack" or for "the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty". Considering that breaches of immigration law are largely treated as criminal offences and that individuals seeking access to the EU by sea may be victims of human trafficking or their lives may be endangered due to unseaworthy vessels, it is likely that any of these exceptions could be (mis-)used to justify mass biometric surveillance of third-country nationals. Article 5(3) requires prior authorisation by a judicial authority or an independent administrative authority, which is an important safeguard, but it remains to be seen which authorities can be involved in this respect; for example, to my mind, a police authority should not qualify as an independent administrative authority.

Of Exceptions and Loopholes

Apart from the problematic categorisation of high-risk AI systems, there exist additional reasons why the AI Act poses challenges to the protection of fundamental rights and the rule of law. Its Article 6(3) enables providers to self-assess their AI system as not falling within the high-risk category. Such exemption may be applied to AI systems intended to perform a narrow procedural task or improve the result of a previously completed human activity, detect decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review, or perform a preparatory task. This exception does not apply to AI systems that perform profiling of natural persons. Providers must document their assessment, register the AI system in the EU database in accordance with Article 49 and provide documents of its assessment to national

competent authorities upon request. The extent to which providers will make extensive use of this exception clause remains to be seen, but it is likely that most AI systems in this field will be treated as not posing a high risk. Importantly, this self-assessment is linked to the *ex ante* conformity assessment that, can take place through two procedures; internal or through an external body (notified body), which is mandatory in limited cases. The field of migration, asylum and border is not one of them and providers shall follow the conformity assessment procedure based on internal control, which does not provide for the involvement of a notified body (Article 43(2)). An internal assessment not only confers significant discretion to providers but also does not safeguard the rule of law, whereby accountability constitutes a significant component (for an analysis, see here and here). Interestingly, the European Parliament had proposed that providers of systems falling under Annex III could submit a reasoned notification to the competent authority if they considered that their system did not pose a significant risk of harm. This does not feature in the AI Act, thus removing an important layer of scrutiny for the classification (see here).

According to the AI Act, high-risk AI systems are subject to a series of requirements and obligations to providers (Sections 2 and 3 of Chapter III). Among these requirements for providers there exists one regarding designing AI systems that enable effective human oversight (Article 14). In relation to biometric identification, no action or decision must be taken by the deployer based on the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority. Recital 73 justifies this high standard by "significant consequences" an incorrect match can have. However, due to specificities of the areas (Recital 73), the requirement for verification by at least two natural persons will not apply to high-risk AI systems in law enforcement, migration, border control, or asylum, when deemed disproportionate under EU or national law. There is no explanation of these specificities or when this requirement might be deemed disproportionate. Besides, it fails to acknowledge that incorrect matches in this field can have significant implications, such as denial of international protection or visas, detention, or return to their country of origin or a third country.

Another requirement which applies to both providers and deployers concerns the registration of high-risk AI systems to the EU database foreseen in Article 71. According to Article 49, whereas most registrations will be publicly available to ensure transparency, high-risk AI systems in migration, asylum, and border control management (along with those on law enforcement) will be registered in a "secure non-public section of the EU database", accessible only to the Commission and national authorities. Furthermore, central information, such as training data used or a summary of the fundamental rights impact assessment, need not to be entered at all (Article 49(4)). These exceptions apply equally to AI systems for both law enforcement and migration, which is reflective of a highly securitised approach fusing the two fields. This fusion entails double standards for third-country nationals, legitimising opacity and leaving them with vague – if any – knowledge of how decisions are made. Such knowledge is a pre-requisite for meaningfully contesting potentially discriminatory or Fundamental rights-violating outcome.

The Curious Case of Article 111 of the AI Act

Finally, according to Article 111 of the AI Act, AI systems forming components of large-scale IT systems in use before 2 August 2027 must comply with this Regulation by 31 December 2030. These involve the operational Schengen Information System (SIS), Visa Information System (VIS), Eurodac and the forthcoming Entry/Exit System (EES), European Travel Information and Authorisation System (ETIAS) and European Criminal Record Information System for Third-country Nationals (ECRIS-TCN), along with interoperability components (Regulations (EU) 2019/817 and 2019/818). The AI Act requirements must be taken into account in the evaluation of each IT system. At the behest of the European Parliament, the final text mandates phased integration of IT systems under the

AI Act by 2030. This is understandable, given the interoperability architecture is still under construction and expected to be fully operational by 2027. With the AI Act becoming applicable in 2026, a three-year deadline for bringing the systems in line with its requirements. This allows AI-powered algorithms in interoperable IT systems, for example for algorithmic risk profiling in ETIAS and VIS, facial recognition or multiple identity detection, can continue as planned (see here). Coupled with the transparency exceptions mentioned earlier, the lack of transparency may remain,. For example, as stressed by Karaiskou in her PhD research, one of the interoperability components, the Common Repository for Reporting and Statistics (CRRS), is likely to use AI tools in the compilation of tailor-made, cross-system statistical data and analytical reporting for policy, operational and data quality purposes. Since this data is anonymised under Article 39 of the Interoperability Regulations, it does not qualify as personal data and thus escapes EU data protection law, including oversight by national supervisory authorities and the European Data Protection Supervisor (EDPS). Delaying the AI Act's application also delays oversight these of AI tools. The result will be that the CRRS may not be subject to any supervision, either from the perspective of EU data protection law or from the AI Act until 2030. This accountability gap is particularly significant, leaving the CRRS potentially functioning as a regulatory black site for several years.

Conclusion

This blog aimed to provide a concise overview of the main problematic issues in relation to the regulation of AI systems in the field of migration, asylum and border management by the AI Act. The analysis has demonstrated that through significant misclassifications, exceptions and loopholes, a differentiated, securitised approach towards migrants and refugees shielded from public scrutiny is legitimised and sustained. One can only hope that supervision through the market surveillance authorities and judicial intervention will shed light upon AI-driven migration technologies, acknowledge the significant impact these systems have on individuals and call for raising the standards for protection. The AI Act is just the beginning.

The author is grateful to Hannah Husser for her valuable analysis within the content of the Odysseus Executive Master at ULB.

ABOUT THE AUTHOR

Niovi Vavoula

Niovi Vavoula is an Associate Professor and holds the Chair in Cyber Policy at the University of Luxembourg.Niovi Vavoula is an Associate Professor and holds the Chair in Cyber Policy at the University of Luxembourg.

SUGGESTED CITATION

Vavoula, Niovi: Regulating AI at Europe's Borders: Where the AI Act Falls Short, Verfassungsblog, 13.12.2024, doi: 10.59704/10a27137a898fa42.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20241213-225632-0.